

Маршрутизаторы Dynamix UM-S

Руководство пользователя



Содержание

Поздравляем!

Вы входите в мир G.shdsl технологий. Ваш новый маршрутизатор - это внешнее G.shdsl устройство, которое легко подключается к компьютеру, коммутатору или концентратору. Маршрутизатор подсоединяется непосредственно к телефонной линии через стандартный телефонный разъем RJ-11.

Описание



SHDSL (Single-Paired High Speed Digital Subscriber Loop) маршрутизатор Dynamix UMS соответствует стандарту G.992.2 с интерфейсом 10/100 Base-T с автосогласованием. Он обеспечивает передачу данных со скоростями от 192Kbps до 2.304Mbps в линии по существующей двухпроводной линии. Устройство способно не только передавать данные, но и служить в качестве моста/маршрутизатора с поддержкой функций Multi-DMZ, virtual server mapping и является прозрачным для VPN туннелей.
Маршрутизатор Dynamix UMSF поддерживает дополнительно функции firewall, SPI, NAT, DoS protection и может служить как полноценный firewall для обеспечения защищенных соединений с внешними пользователями.
Маршрутизаторы Dynamix UMS4 и UMS4F дополнительно содержат встроенный 4хпортовый 10Base-T /100Base-T коммутатор с автосогласованием.
Это семейство позволяет пользователям внедрить последние достижения широкополосных технологий, чтобы удовлетворить свои быстро растущие коммуникационные потребности. Используя это семейство, Вы получаете доступ к полной надежности и управляемости оборудования.

Характеристики

- Легкое конфигурирование и управление в различных приложениях с использованием защиты по паролю
- Эффективная IP маршрутизация и режим прозрачного обучаемого моста для поддержания широкополосных Интернет услуг
- Поддержка VPN туннелей для защищенных соединений
- Встроенный расширенный SPI firewall (UMSF/UMS4F только)
- 4х портовый коммутатор 10/100Mbps с автосогласованием и Auto-MDIX для облегчения создания LAN (UMS4/UMS4F)
- DMZ host/Multi-DMZ/Multi-NAT позволяет всем рабочим станциям использовать один IP адрес для доступа в Интернет
- Поддержка ATM протоколов поверх SHDSL (ATMoSHDSL)
- В режимах PPPoA и PPPoE поддерживается аутентификация пользователя через PAP/CHAP/MS-CHAP
- SNMP управление через SNMPv1/SNMPv2 агент и MIB II
- Дополнение новых возможностей посредством модификации встроенного программного обеспечения

Спецификация

Routing

- Поддержка протоколов IP/TCP/UDP/ARP/ICMP/IGMP
- Маршрутизация: статическая и RIPv1/RIPv2 (RFC1058/2453)
- IP multicast и IGMP proxy (RFC1112/2236)
- Трансляция сетевых адресов (NAT/PAT) (RFC1631)
- NAT ALGs для ICQ/Netmeeting/MSN/Yahoo Messenger
- DNS relay и caching (RFC1034/1035)
- Сервер DHCP (RFC2131/2132)

Мост:

- IEEE 802.1D прозрачный обучающийся мост

Безопасность:

- DMZ host/Multi-DMZ/Multi-NAT function
- Virtual server mapping (RFC1631)
- VPN pass-through for PPTP/L2TP/IPSec tunneling
- NAT firewall
- Расширенный Stateful packet inspection (SPI) firewall (UMSF/UMS4F)
- Шлюз уровня приложений для блокировки URL (UMSF/UMS4F)
- Управление доступом пользователей: запрет определенным компьютерам вход в Интернет (UMSF/UMS4F)

Управление:

- Легкоосваиваемый web-интерфейс GUI для быстрой установки, конфигурирования и управления
- Меню-ориентированный интерфейс/Интерфейс командной строки (Command-line interface CLI) для управления с консоли или через Telnet
- Администрируемый по паролю список контроля доступа и управления
- SNMP управление через SNMPv1/SNMPv2c (RFC1157/1901/1905) агент и MIB II (RFC1213/1493)
- Обновление ПО через web-броузер/TFTP сервер

ATM

- До 8 PVCs
- Поддержка UBR/CBR/VBR
- OAM F5 AIS/RDI и петли
- AAL5

AAL5 Encapsulation

- VC multiplexing and SNAP/LLC
- Ethernet over ATM (RFC 2684/1483)
- PPP over ATM (RFC 2364)
- Классический IP over ATM (RFC 1577)

PPP

- PPP over Ethernet (RFC 2516)
- PPP over ATM (RFC 2364)
- Аутентификация пользователя по PAP/CHAP/MS-CHAP

WAN Интерфейс

- SHDSL: ITU-T G.991.2 (Annex A, Annex B)
- Кодовая схема: 16-TCPAM
- Скорость передачи данных: N x 64Kbps (N=1~36)
- Impedance: 135 ohms

LAN Интерфейс

- 4-коммутатор (UMS4/UMS4F)
- 10 Base-T and 100 Base-T с автосогласованием
- Auto-MDIX (UMS4/UMS4F)

Аппаратный Интерфейс

- WAN: RJ-11
- LAN: RJ-45 x 4 (UMS4/UMS4F) или RJ-45 x 1 (UMS/UMSF)
- Консольный порт: RS232

Индикаторы:

- PWR
- WAN: LNK, ACT
- LAN: 10M/ACT, 100M/ACT, ALM (UMS/UMSF)
- LAN: 1, 2, 3, 4, ALM (UMS4/UMS4F)

Физические/электрические параметры:

- Размеры: 18.7 x 3.3 x 14.5cm (WxHxD)

- Питание: 100~240VAC (через блок питания)
- Потребление: 6 Ватт
- Рабочая температура: 0~45 С
- Рабочая влажность: 0%~95%RH (неконденсируемая)

Память

- 2MB Flash Memory, 4MB SDRAM

Состав серии Dynamix UMS:

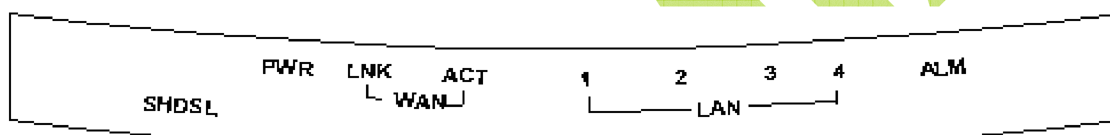
UMS - G.shdsl маршрутизатор с 1 LAN-портом
UMSF - G.shdsl маршрутизатор с 1 LAN-портом и firewall
UMS4 - G.shdsl маршрутизатор с 4 LAN-портами
UMS4F - G.shdsl маршрутизатор с 4 LAN-портами и firewall

Начальные сведения

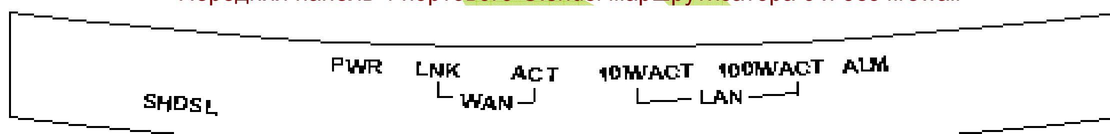
В этой секции мы рассмотрим как аппаратно выглядит маршрутизатор.

Передняя панель

На передней панели расположены светодиодные индикаторы



Передняя панель 4 портового G.shdsl маршрутизатора с и без firewall



Передняя панель 1 портового G.shdsl маршрутизатора с и без firewall

Индикаторы на 4х-портовом маршрутизаторе

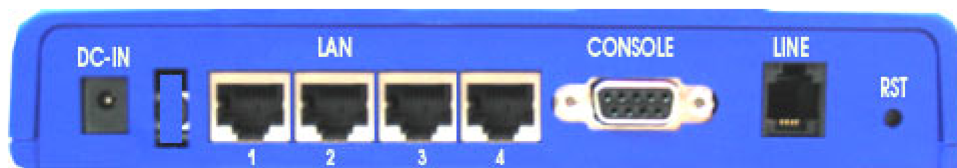
Наименование		Состояние	Описание
PWR		Вкл	Питание подано на устройство
WAN	LNK	Вкл	SHDSL соединение установлено
	ACT	Вкл	Идет передача или получение информации через SHDSL линию
LAN	1	Вкл	Идет передача или получение информации через порт LAN 1
	2	Вкл	Идет передача или получение информации через порт LAN 2
	3	Вкл	Идет передача или получение информации через порт LAN 3
	4	Вкл	Идет передача или получение информации через порт LAN 4
ALM		Вкл	SHDSL соединение разорвано

Индикаторы на 1-портовом маршрутизаторе

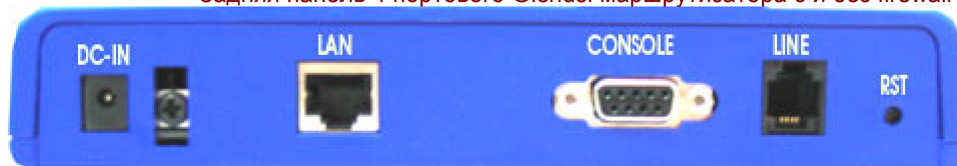
PWR		Вкл	Питание подано на устройство
WAN	LNK	Вкл	SHDSL соединение установлено
	ACT	Вкл	Идет передача/получение информации через SHDSL линию
LAN	10M/ACT	Вкл	LAN порт в режиме 10M
	100M/ACT	Вкл	LAN порт в режиме 100M
ALM		Вкл	SHDSL соединение разорвано

Задняя панель

На задней панели осуществляются все подсоединения.



Задняя панель 4 портового G.shdsl маршрутизатора с и без firewall



Задняя панель 1 портового G.shdsl маршрутизатора с и без firewall

**ВНИМАНИЕ: В целях пожаробезопасности, используйте для подсоединения к телефонной линии кабель с диаметром не менее 0,5 мм**

Описание разъемов для 1-портового устройства

DC-IN	Разъем для подключения блока питания: Входное напряжение 9VDC
LAN	Гнездо для подключения Ethernet 10BaseT (RJ-45)
CONSOLE	RS- 232C (DB9) для системной конфигурации и обслуживания
LINE	WAN порт для SHDSL линии (RJ-11)
RST	Кнопка восстановления конфигурации по умолчанию

Описание разъемов для 4хпортового устройства

DC-IN	Разъем для подключения блока питания: Входное напряжение 9VDC
LAN (1,2,3,4)	LAN порт :10/100BaseT с автоопределением и авто-MDIX (RJ-45)
CONSOLE	RS- 232C (DB9) для системной конфигурации и обслуживания
LINE	WAN порт для SHDSL линии (RJ-11)

Конфигурирование маршрутизатора

Этот раздел поможет пользователю наиболее легким и быстрым способом настроить свое устройство используя WEB-интерфейс. Пожалуста, точно следуйте инструкциям.

Примечание: Существуют три метода конфигурирования маршрутизатора: консольный порт, Telnet и Web браузер. Эти методы не могут использоваться одновременно.
При использовании Web конфигурирования, пропустите шаги 1 и 2
Для конфигурирования через консоль, пропустите шаг 3.

Шаг 1: Проверьте наличие Ethernet адаптера

Удостоверьтесь, что Ethernet адаптер установлен в Вашем компьютере или ноутбуке. Поскольку при Web конфигурировании используется TCP/IP протокол, проверьте что он установлен.

Шаг 2: Проверьте наличие программы терминального доступа

Для конфигурирования через консоль либо Telnet требуется наличие программы терминального доступа с эмуляцией терминала типа VT100.

Шаг 3: Проверьте наличие Web браузера

Для Web конфигурирования у Вас должен быть установлен какой-либо Web браузер, например IE или Netscape.
Примечание:Рекомендуем IE5.0, Netscape 6.0 или выше и разрешение 800x600 или выше.

Шаг 4: Определите параметры соединения

Выберите Интернет протокол по которому Вы будете связываться и определите режим работы.

Выбор протокола

RFC1483	Bridged Ethernet over ATM

RFC1577 Classical Internet Protocol over ATM
RFC2364 Point-to-Point Protocol over ATM
RFC2516 Point-to-Point Protocol over Ethernet

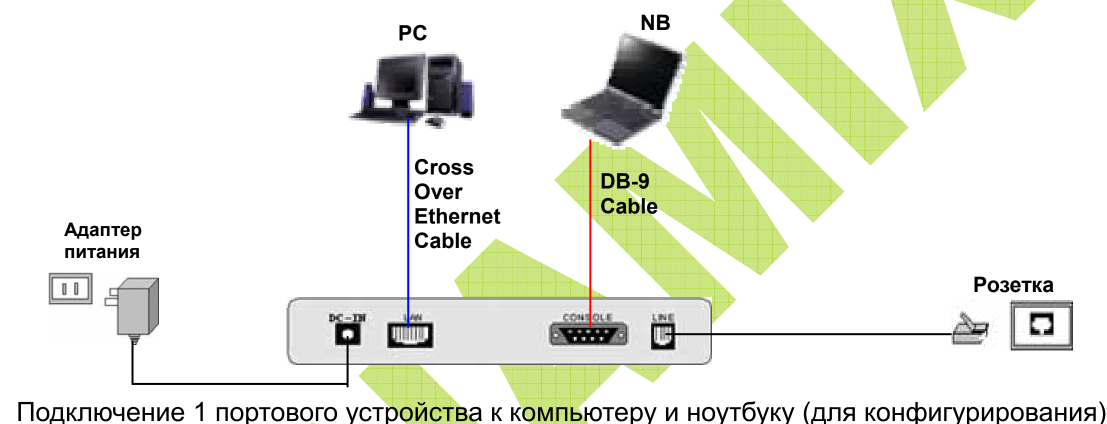
Шаг 5: Установка SHDSL маршрутизатора

Внимание: Во избежание повреждения устройства, не включайте питание пока не установите его полностью.

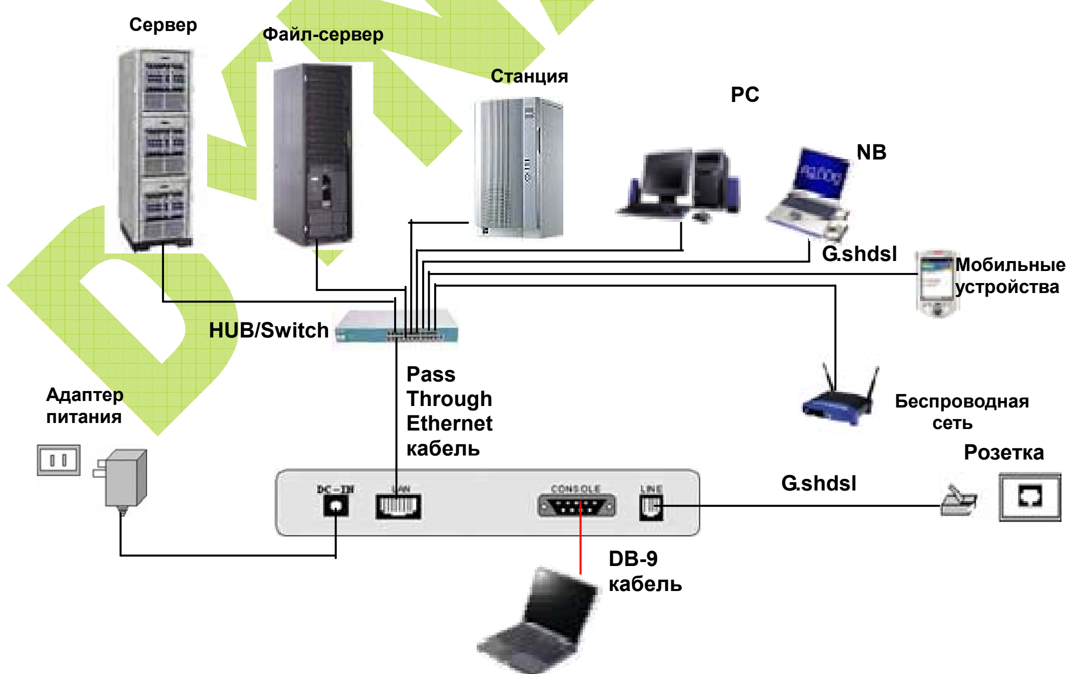
✓ Подсоедините кабель питания к порту DC-IN расположенному на задней панели.
✓ Подсоедините Ethernet кабель.

Если 1 портовое устройство подсоединяется непосредственно к компьютеру, то используется "cross over" кабель. В случае подключения к концентратору или коммутатору, сначала убедитесь поддерживает ли он режим автоопределения. Если да, то можно использовать и "cross over" и "pass through" кабеля. Если же нет, то только "pass through" Ethernet кабель должен использоваться. 4х портовый маршрутизатор поддерживает авто-MDIX порты, поэтому можно использовать любой кабель.

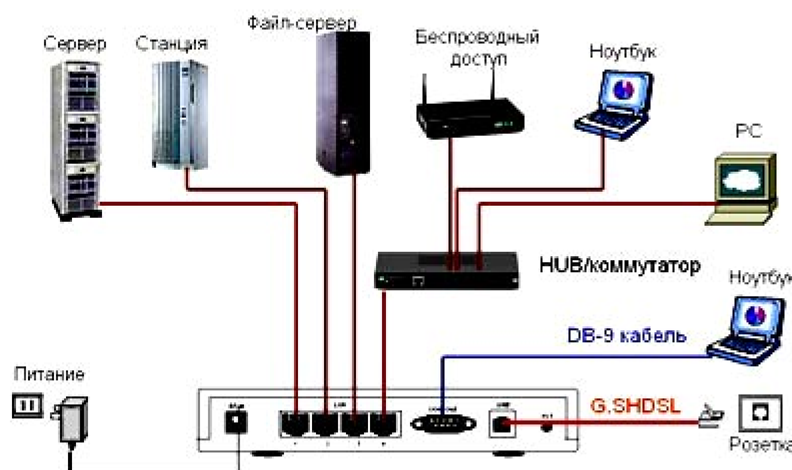
✓ Подсоедините телефонный кабель к устройству, а противоположный конец к телефонной розетке.
✓ Подсоедините кабель питания к электрической розетке.
✓ Включите компьютер, который будет использоваться для конфигурирования.



Подключение 1 портового устройства к компьютеру и ноутбуку (для конфигурирования)



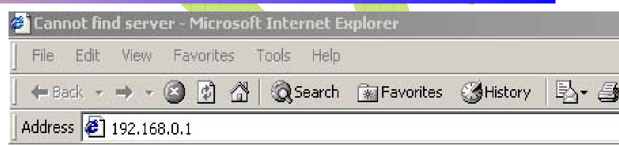
Подключение 1 портового устройства к концентратору/коммутатору



4х-портовое устройство в офисной сети

Конфигурация с использованием Web Browser

Откройте IE или Netscape браузер для доступа к устройству. Наберите http://192.168.0.1. IP адрес и sub net-mask по умолчанию: 192.168.0.1 и 255.255.255.0. Поскольку маршрутизатор выступает как DHCP сервер в Вашей сети, он автоматически назначит IP адрес для компьютера.



Наберите имя пользователя root и пароль root , затем нажмите OK.
Это значения по умолчанию.
Рекомендуем изменить их после завершения конфигурирования.

Примечание: После изменения имени и пароля рекомендуем их сохранить, поскольку их Вы будете использовать в следующих сеансах.

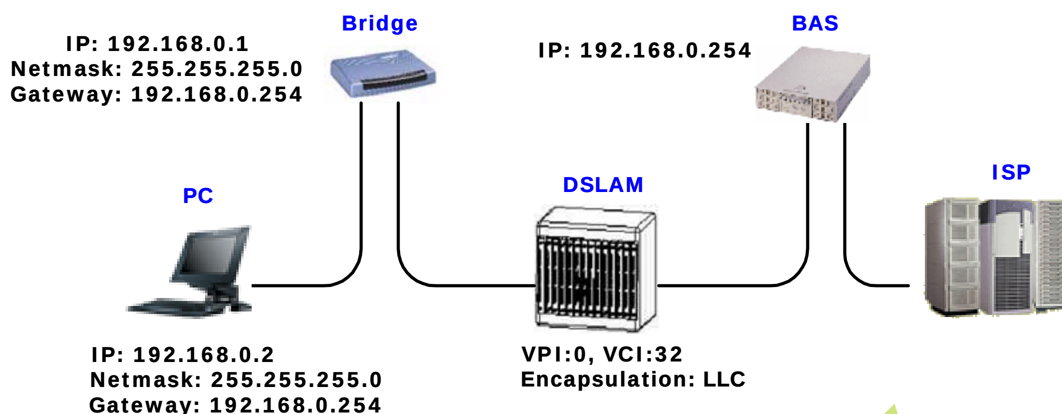


Basic Setup

Basic Setup служит для установки параметров режимов маршрутизации и моста.
Нажмите Basic для установки.



Bridge Mode



Выберите Bridge и CPE Side для установки режима моста и нажмите Next для продолжения

Home | Basic | Advanced | Status | Admin | Utility

BASIC - STEP1

Operation Mode:

System Mode: ROUTE BRIDGE
SHDSL Mode: CO Side CPE Side

Cancel Reset Next

Параметры LAN
Введите IP: 192.168.0.1
Введите Subnet Mask: 255.255.255.0
Введите Gateway: 192.168.0.254
Введите Host Name: SOHO

Параметры WAN1
Введите VPI: 0
Введите VCI: 32
Нажмите LLC
Нажмите Next.

Home | Basic | Advanced | Status | Admin | Utility

BASIC - STEP2

LAN:

IP Address: 192 . 168 . 0 . 1
Subnet Mask: 255 . 255 . 255 . 0
Gateway: 192 . 168 . 0 . 254
Host Name: SOHO

WAN1:

VPI: 0
VCI: 32
Encap.: VC-mux LLC

Back Cancel Reset Next

Экран будет отображать вновь введенные параметры. Проверьте их и нажмите Restart. После перезагрузки будут активизированы новые значения. Нажмите Continue если Вы хотите продолжить конфигурирование.

Routing Mode

Routing mode содержит: DHCP server, Point-to-Point Protocol over ATM и Ethernet, IP over ATM и Ethernet over ATM. Вы должны установить протокол, используемый Вашим ISP.
Нажмите ROUTE and CPE Side, а затем Next.

Home | Basic | Advanced | Status | Admin | Utility

BASIC - STEP1

Operation Mode:

System Mode: ROUTE BRIDGE
SHDSL Mode: CO Side CPE Side

Cancel Reset Next

Введите параметры LAN :
IP Address: 192.168.0.1
Subnet Mask: 255.255.255.0
Host Name: SOHO
DHCP Service: Enable
По умолчанию выбрано: Enable DHCP server. Если хотите его выключить, выберите Disable.

Home | Basic | Advanced | Status | Admin | Utility

BASIC - STEP2

LAN:

IP Address: 192 . 168 . 0 . 1
Subnet Mask: 255 . 255 . 255 . 0
Host Name: SOHO
Trigger DHCP Service: Disable Enable

Back Cancel Reset Next

DHCP Server

Dynamic Host Configuration Protocol (DHCP) это коммуникационный протокол, который позволяет администратору сети централизованно управлять и автоматизировать выделение IP адресов в сети предприятия. Каждая машина, подсоединенная к Интернету должна иметь уникальный IP адрес.
Без DHCP, IP адрес должен вводится вручную на каждом компьютере. Если компьютер перемещается в другой сегмент сети, его IP адрес должен быть изменен. DHCP позволяет сетевому администратору отслеживать и назначать IP адреса централизованно, т.е. автоматически посылать новый IP адрес, когда где-либо подключается новый компьютер.

Если DHCP сервер разрешен, Вы должны установить следующие параметры для его функционирования.

Учтите, что DHCP сервер может работать максимум с 253 пользователями Интернет одновременно.

Пример: Если LAN IP адрес: 192.168.0.1, и используемые IP адреса от 192.168.0.2 до 192.168.0.51. DHCP сервер назначает IP адреса от "Start IP Address" до "End IP Address". Разрешенное пространство IP адресов от 0 до 255, но 0 и 255 зарезервированы для широковещательных посылок, поэтому разрешены IP адреса от 1 до 254. "Lease time" 72 часа показывает, что DHCP сервер переназначает IP каждые 72 часа.

Теперь нажмите Next для установки параметров WAN.

Home | Basic | Advanced | Status | Admin | Utility

BASIC - STEP3

DHCP SERVER:

- General DHCP Parameter:

Start IP Address: 192.168.0. 2
End IP Address: 192.168.0. 51
DNS Server 1: 192.168.0.1
DNS Server 2:
DNS Server 3:
Lease Time: 72 hours

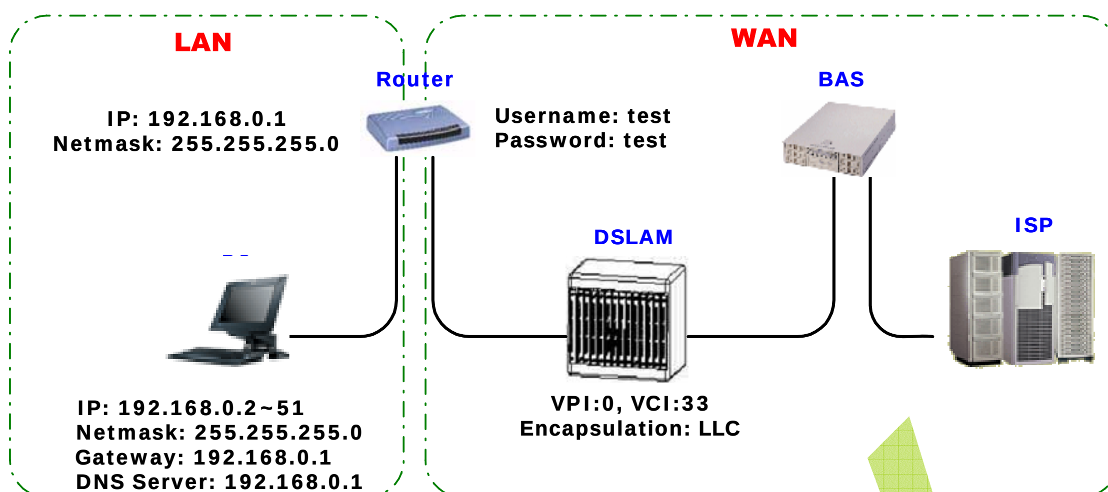
- Table of Fixed DHCP Host Entries:

Index	MAC Address	IP Address
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

Back Cancel Reset Next

PPPoE or PPPoA

PPPoA (point-to-point protocol over ATM) и PPPoE (point-to-point protocol over Ethernet) это протоколы аутентификации и соединений используемые многими провайдерами для широкополосного доступа в Интернет. Это спецификации для подсоединения нескольких компьютеров одной локальной сети к удаленному узлу через совместно используемое устройство (CPE). PPPoE и PPPoA можно использовать в офисе или здании. Пользователи используют одну DSL линию, кабельный модем или беспроводное соединение для подключения к Интернет. PPPoE и PPPoA совмещают PPP, наиболее часто используемый в коммутируемом доступе с Ethernet или ATM протоколом, который поддерживает многих пользователей в локальной сети. Информация PPP протокола включается в состав Ethernet или ATM пакетов (фреймов).



Введите параметры WAN1:
VPI: 0
VCI: 33
AAL5 Encap: LLC
Protocol: PPPoA + NAT или PPPoE + NAT
Нажмите Next для установки "User name" и "Password".

Для понимания NAT, смотрите страницу 19.

Home | Basic | Advanced | Status | Admin | Utility

BASIC - STEP4

WAN1:
VPI: 0
VCI: 32
AAL5 Encap: VC-mux LLC
Protocol: IPoA
IPoA
IPoA+NAT
EoA
EoA+NAT
PPPoA+NAT
PPPoE+NAT
Back Cancel Reset Next

Введите параметры ISP1
Имя пользователя и пароль предоставляются Вашим ISP
Username: test
Password: test
Password Confirm: test
Idle Time: 10
Нажмите Next.
В целях безопасности пароль будет отображаться звездочками.

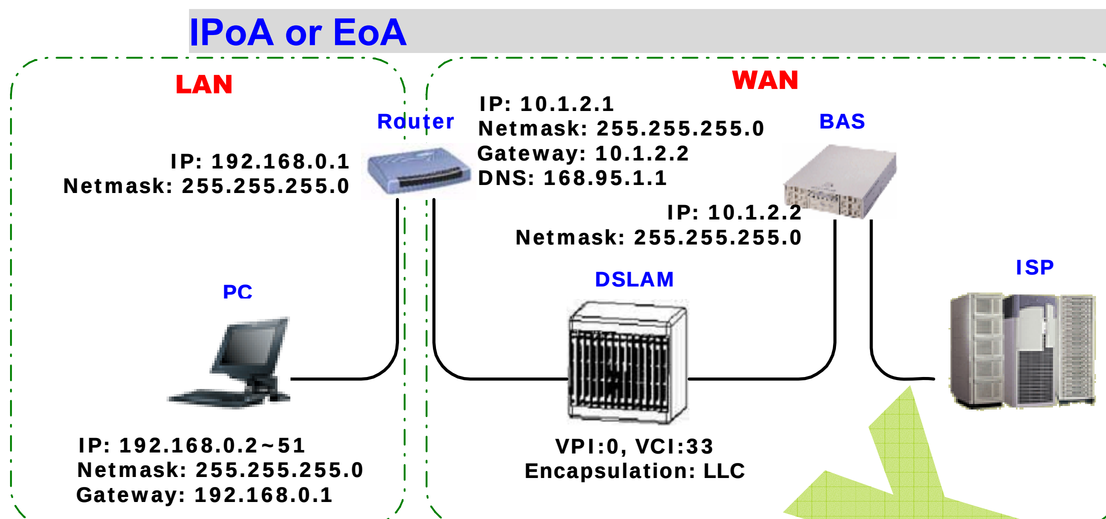
Home | Basic | Advanced | Status | Admin | Utility

BASIC - STEP5

ISP1:
Username: test
Password: ****
Password Confirm: ****
Idle Time: 10 minutes
Back Cancel Reset Next

На экране отображаются параметры, которые будут записаны в EPROM. Проверьте их перед записью. Нажмите Restart для перезапуска и активизации новых параметров или Continue для продолжения установки.

IPoA or EoA



Введите параметры WAN;
VPI: 0
VCI: 33
AAL5 Encap: LLC
Protocol: IPoA , EoA , IPoA + NAT или EoA + NAT
Нажмите Next и перейдите к установке параметров IP

Для понимания NAT, смотрите страницу 19.

Home Basic Advanced Status Admin Utility
BASIC - STEP4
WAN1:
VPI: 0
VCI: 32
AAL5 Encap: VC-mux LLC
Protocol: IPoA
IPoA
IPoA+NAT
EoA
EoA+NAT
PPPoA+NAT
PPPoE+NAT
Back Cancel Reset Next

IP Address: 10.1.2.1
Subnet mask: 255.255.255.0
Gateway: 10.1.2.2
DNS Server 1: 168.95.1.1
Нажмите Next

Home Basic Advanced Status Admin Utility
BASIC - STEP5
WAN1:
IP Address: 10 . 1 . 2 . 1
Subnet Mask: 255 . 255 . 255 . 0
Gateway: 10 . 1 . 2 . 2
DNS Server 1: 168.95.1.1
DNS Server 2:
DNS Server 3:
Back Cancel Reset Next

На экране отображаются параметры, которые будут записаны в EPROM. Проверьте их перед записью. Нажмите Restart для перезапуска и активизации новых параметров или Continue для продолжения установки.

Поздравляем! Вы закончили.
Ваше SHDSL Интернет соединение установлено!

Расширенная установка

Расширенная установка позволяет задать параметры SHDSL, WAN, Bridge, Route, NAT/DMZ, Virtual server и firewall.



SHDSL

Вы можете выбрать тип Annex, скорость и значение SNR для параметров SHDSL.
Нажмите SHDSL



Тип Annex: Существуют два типа Annex, Annex A и Annex B в SHDSL.
Скорость данных: можно установить с шагом 64kbps.
Значение SNR margin: от 0 до 10.
: В общем случае, значение SNR не требуется менять, поскольку это затрагивает скорость.

Home | Basic | Advanced | Status | Admin | Utility

ADVANCED - SHDSL

Operation Mode:

- Setup Operation Mode:
  - Annex Type: Annex A / Annex B
  - Data Rate(n*64kbps): 0 (range:0~36, n=0 for adaptive mode)
  - SHDSL SNR margin: 0 (range:0~10)

Cancel | Reset | Finish

На экране отображаются параметры, которые будут записаны в EPROM. Проверьте их перед записью. Нажмите Restart для перезапуска и активизации новых параметров или Continue для продолжения установки.

WAN

SHDSL маршрутизатор поддерживает до 8 PVC. Параметры устанавливаются в WAN.



WAN номер 1 задается при базовой установке. Если Вы хотите добавить PVC, вы должны сконфигурировать от WAN 2 до WAN 8.

Введите необходимые параметры.

Home | Basic | Advanced | Status | Admin | Utility

ADVANCED - WAN

WAN Interface Parameters:

- **Table of Current WAN Interface Parameter:**

No	WAN			VC					ISP			
	Protocol	IP Address	Subnet Mask	VPI	VCI	AAL5 Encap	QoS Class	QoS PCR	Username	Password	Password Confirm	Idle Time
1	IP over ATM	10.1.2.1	255.255.255.0	0	32	LLC	UBR	2400	test	****	****	10
2	Disable	192.168.2.1	255.255.255.0	0	33	LLC	UBR	2400	test	****	****	10
3	Disable	192.168.3.1	255.255.255.0	0	34	LLC	UBR		test	****	****	10
4	Disable	192.168.4.1	255.255.255.0	0	35	LLC	UBR	2400	test	****	****	10
5	Disable	192.168.5.1	255.255.255.0	0	36	LLC	UBR	2400	test	****	****	10
6	Disable	192.168.6.1	255.255.255.0	0	37	LLC	UBR	2400	test	****	****	10
7	Disable	192.168.7.1	255.255.255.0	0	38	LLC	UBR	2400	test	****	****	10
8	Disable	192.168.8.1	255.255.255.0	0	39	LLC	UBR	2400	test	****	****	10

Cancel | Reset | Finish

Нажмие Finish для завершения.

На экране отображаются параметры, которые будут записаны в EPROM. Проверьте их перед записью. Нажмите Restart для перезапуска и активизации новых параметров или Continue для продолжения установки.

Bridge

Режим моста устанавливается заданием статических параметров.

Нажмите Bridge для установки.

BASIC
ADVANCED
- SHDSL
- WAN
- BRIDGE
- ROUTE
- NAT/DMZ
- VIRTUAL SERVER
- FIREWALL

STATUS
ADMIN
UTILITY

Нажмите Add, чтобы ввести требуемую информацию.

Home | Basic | Advanced | Status | Admin | Utility

ADVANCED - BRIDGE

Generic Bridge Parameters:

- General Parameter:

Default Gateway: 192.168.0.254

Static Bridge Parameters:

- Table of Current MAC Entries:

No	MAC Address	LAN	WAN1 - 4	WAN5 - 8
1	00:00:00:00:00:00	Filter	1. Filter 2. Filter 3. Filter 4. Filter	5. Filter 6. Filter 7. Filter 8. Filter

Add

Cancel Finish

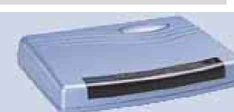
На экране отображаются параметры, которые будут записаны в EPROM. Проверьте их перед записью. Нажмите Restart для перезапуска и активизации новых параметров или Continue для продолжения установки.

Route

Если маршрутизатор подключен более чем к одной сети, возникает необходимость задать статические маршруты между ними. Статический маршрут - это заранее определенный путь по которому информация будет следовать к определенному узлу или сети.

При динамической маршрутизации Вы позволяете маршрутизатору отслеживать изменения в сети. Используя RIP протокол, маршрутизатор определяет путь на основании наименьшего числа прыжков (hops) между точкой отправления и назначения. Также RIP протокол инициирует регулярный обмен требуемой информацией между узлами сети.

Нажмите Route для задания параметров маршрутизации.



- ► BASIC
- ▼ ADVANCED
  - SHDSL
  - WAN
  - BRIDGE
  - ROUTE
  - NAT/DMZ
  - VIRTUAL SERVER
  - FIREWALL
- ► STATUS
- ► ADMIN
- ► UTILITY

Home | Basic | Advanced | Status | Admin | Utility

ADVANCED - ROUTE

Static Route and RIP Parameters:

- Table of Current Static Route Entries:

Index	Network Address	Subnet Mask	Gateway
⊙ 1	0.0.0.0	0.0.0.0	10.1.2.2
2			

Add | Delete | Modify | Reset

- General RIP Parameter:

RIP Mode: ⊙ Disable ○ Enable
Auto RIP Summary: ⊙ Disable ○ Enable

- Table of Current Interface RIP Parameter:

Interface	RIP Mode	Version	Authentication Required	Poison Reverse	Authentication Code
⊙ LAN	Disable	2	None	Enable	None
○ WAN1	Disable	2	None	Enable	None
○ WAN2	Disable	--	None	Disable	None
○ WAN3	Disable	--	None	Disable	None

Для изменения параметров RIP (Routing information protocol):
RIP Mode: Enable
Auto RIP Summary: Enable
Нажмите Modify

Home | Basic | Advanced | Status | Admin | Utility

- General RIP Parameter:

RIP Mode: ○ Disable ⊙ Enable
Auto RIP Summary: ○ Disable ⊙ Enable

- Table of Current Interface RIP Parameter:

Interface	RIP Mode	Version	Authentication Required	Poison Reverse	Authentication Code
⊙ LAN	Disable	2	None	Enable	None
○ WAN1	Disable	2	None	Enable	None
○ WAN2	Disable	--	None	Disable	None
○ WAN3	Disable	--	None	Disable	None
○ WAN4	Disable	--	None	Disable	None
○ WAN5	Disable	--	None	Disable	None
○ WAN6	Disable	--	None	Disable	None
○ WAN7	Disable	--	None	Disable	None
○ WAN8	Disable	--	None	Disable	None

Modify

RIP Mode: этот параметр определяет как будет отрабатываться RIP (Routing information protocol). RIP позволяет обмениваться информацией с другими маршрутизаторами. Если установлено "Disable", устройство не будет участвовать в RIP обмене с другими. Если же "Enable", маршрутизатор будет рассылать свою таблицу маршрутизации и добавлять в нее информацию полученную от других. Если установить "Silent", устройство не будет рассылать , но будет добавлять.

▪ Table of Current Interface RIP Parameter:

Interface	RIP Mode	Version	Authentication Required	Poison Reverse	Authentication Code
LAN	Disable (Disable / Enable / Silent)	2	None	Enable	
WAN1		2	None	Enable	None
WAN2		--	None	Disable	None
WAN3	Disable	--	None	Disable	None
WAN4	Disable	--	None	Disable	None
WAN5	Disable	--	None	Disable	None
WAN6	Disable	--	None	Disable	None
WAN7	Disable	--	None	Disable	None
WAN8	Disable	--	None	Disable	None

Cancel Ok Reset

RIP Version: определяет формат и метод рассылки RIP сообщений.
RIP v1: посылать только RIP v1 сообщения.
RIP v2: посылать RIP v2 сообщения в формате multicast и broadcast.

▪ Table of Current Interface RIP Parameter:

Interface	RIP Mode	Version	Authentication Required	Poison Reverse	Authentication Code
LAN	Disable	2 (1 / 2)	None	Enable	
WAN1	Disable		None	Enable	None
WAN2	Disable	--	None	Disable	None
WAN3	Disable	--	None	Disable	None
WAN4	Disable	--	None	Disable	None
WAN5	Disable	--	None	Disable	None
WAN6	Disable	--	None	Disable	None
WAN7	Disable	--	None	Disable	None
WAN8	Disable	--	None	Disable	None

Cancel Ok Reset

Authentication required.
None: для RIP не требуется кода аутентификации.
Password: RIP защищается паролем.
MD5: RIP сначала декодируется MD5, затем защищается паролем.

▪ Table of Current Interface RIP Parameter:

Interface	RIP Mode	Version	Authentication Required	Poison Reverse	Authentication Code
LAN	Disable	2	None (None / Password / MD5)	Enable	
WAN1	Disable	2		Enable	None
WAN2	Disable	--		Disable	None
WAN3	Disable	--	None	Disable	None
WAN4	Disable	--	None	Disable	None
WAN5	Disable	--	None	Disable	None
WAN6	Disable	--	None	Disable	None
WAN7	Disable	--	None	Disable	None
WAN8	Disable	--	None	Disable	None

Cancel Ok Reset

"Poison Reserve" используется для определения рассылки RIP информации при изменении маршрута (например: не функционирует один из маршрутизаторов).
Enable: устройство будет активно рассылать информацию.
Disable: рассылки информации не будет.

▪ Table of Current Interface RIP Parameter:

Interface	RIP Mode	Version	Authentication Required	Poison Reverse	Authentication Code
LAN	Disable	2	None	Enable (Disable / Enable)	
WAN1	Disable	2	None		None
WAN2	Disable	--	None	Disable	None
WAN3	Disable	--	None	Disable	None
WAN4	Disable	--	None	Disable	None
WAN5	Disable	--	None	Disable	None
WAN6	Disable	--	None	Disable	None
WAN7	Disable	--	None	Disable	None
WAN8	Disable	--	None	Disable	None

Cancel Ok Reset

После изменения параметров RIP, нажмите Finish.
На экране отображаются параметры, которые будут записаны в EPROM. Проверьте их перед записью. Нажмите Restart для перезапуска и активизации новых параметров или Continue для продолжения установки.

NAT/DMZ



- BASIC
- ADVANCED
  - SHDSL
  - WAN
  - BRIDGE
  - ROUTE
  - NAT/DMZ
  - VIRTUAL SERVER
  - FIREWALL
- STATUS
- ADMIN
- UTILITY

NAT (Network Address Translation) служит для преобразования IP адресов, используемых внутри одной сети в адреса, известные внутри другой сети. Первая сеть рассматривается как внутренняя, а вторая - как внешняя. Обычно, осуществляется отображение локальных адресов сети клиента на один или более глобальных внешних IP адресов и эти внешние адреса используются для переадресации входящих пакетов на локальные IP адреса. Это усиливает безопасность, поскольку каждый входящий или выходящий запрос должен проходить процедуру преобразования, что дает возможность распознать запрос или сравнить с предшествующим. NAT также сокращает потребность клиента в глобальных IP адресах, вплоть до использования всего одного адреса.

DMZ (демилитаризованная зона) это компьютер или небольшая сеть, встроенная между часной сетью клиента и внешней общей сетью. Это предотвращает доступ внешних пользователей к ресурсам внутренней частной сети клиента.

В стандартной конфигурации, отдельный компьютер получает запросы от клиентов корпоративной частной сети на доступ к Интернет. Этот DMZ компьютер инициирует сессии с публичной сетью. Однако, он не может инициировать сессию по запросу из публичной сети. Он только пересылает пакеты, которые были запрошены.

Для пользователей публичной сети доступен только DMZ компьютер. DMZ обычно еще содержит Web сервер компании, который также должен быть доступен внешним запросам. Но DMZ не дает доступа к другим ресурсам компании. Даже если внешний пользователь нарушит целостность DMZ, будут повреждены только Web страницы, остальная информация будет сохранена.

Нажмите NAT/DMZ для установки параметров.

Если Вы хотите разрешить функцию NAT/DMZ, выберите Enable. "Enable the DMZ host Function" для какого WAN с IP адресом включена DMZ функция.

Multi-DMZ: Некоторые пользователи используют несколько внешних IP адресов. Таблица служит для преобразования внешних и виртуальных IP адресов.

Multi-NAT: Некоторые из виртуальных IP адресов (например 192.168.0.10 ~ 192.168.0.50) совместно используют два или более внешних IP (например: 69.210.1.9 и 69.210.1.10). Multi-NAT должна быть установлена так:
Virtual Start IP Address: 192.168.0.10
Count: 40
Global Start IP Address: 69.210.1.9
Count: 2

Home | Basic | Advanced | Status | Admin | Utility

ADVANCED - NAT/DMZ

Network Address Translation and DMZ Hosts Parameters:

- NAT/DMZ function:
  - NAT/DMZ Function: Disable Enable
- DMZ Host:
  - DMZ Host Function: Disable Enable
  - Virtual IP Address:
  - Active Interface: WAN1
- Multi-DMZ:

ID	Virtual IP Address	Global IP Address	Interface
1			WAN1
2			WAN1
3			WAN1
4			WAN1
5			WAN1
6			WAN1

Нажмите Finish для продолжения.

На экране отображаются параметры, которые будут записаны в EPROM. Проверьте их перед записью. Нажмите Restart для перезапуска и активизации новых параметров или Continue для продолжения установки.

7			WAN1
8			WAN1
9			WAN1
10			WAN1

- Multi-NAT:

ID	Virtual Start IP Address	Count	Global Start IP Address	Count	Interface
1		0		0	WAN1
2		0		0	WAN1
3		0		0	WAN1
4		0		0	WAN1
5		0		0	WAN1

Cancel Reset Finish

Virtual Server

Пример: Определенные порты WAN интерфейса отображаются на сервисы внутри LAN.В случае, если адрес 69.210.1.8 (полученный для WAN интерфейса от ISP) виден со стороны Интернет, но реально не соответствует ни одному сервису (кроме NAT конечно) запущенному на устройстве, говорят что мы имеем дело с виртуальным сервером. TCP запрос к порту 69.210.1.8:80 должен переадресовываться на server 1 с портом 192.168.0.2:80 в рабочие дни понедельник-пятница с 8 утра до 6 вечера, UDP запросы к 69.210.1.8:25 отсылаются на server 2 порт 192.168.0.3:25 и обслуживатся всегда.



- BASIC
- ADVANCED
  - SHDSL
  - WAN
  - BRIDGE
  - ROUTE
  - NAT/DMZ
  - VIRTUAL SERVER
  - FIREWALL
- STATUS
- ADMIN
- UTILITY

Будем устанавливать маршрутизатор так:
Index 1, протокол TCP, интерфейс WAN1, имя сервиса test1, внутренний IP 192.168.0.2, внутренний порт 80, внешний порт 80, график работы с понедельника по пятницу с 8:00 до 16:00 и index 2, протокол UDP, интерфейс WAN1, имя сервиса test2, внутренний IP 192.168.0.3, внутрений порт 25, внешний порт 25, доступен всегда.

Нажмите Virtual Server для установки параметров.

Нажмите Modify .

Home Basic Advanced Status Admin Utility

ADVANCED - VIRTUAL SERVER

Virtual Server Mapping Parameters:

- Table of Current Virtual Server Entries:

Index	Service Name	Interface	Private IP	Protocol	Schedule
1	---	---	---	Disable	---
2	---	---	---	Disable	---
3	---	---	---	Disable	---
4	---	---	---	Disable	---
5	---	---	---	Disable	---
6	---	---	---	Disable	---
7	---	---	---	Disable	---
8	---	---	---	Disable	---
9	---	---	---	Disable	---
10	---	---	---	Disable	---

Cancel Modify Finish

Введите необходимые параметры, затем нажмите Finish.

Нажмите Restart для перезапуска и активизации новых параметров или Continue для продолжения установки.

Home | Basic | Advanced | Status | Admin | Utility

ADVANCED - VIRTUAL SERVER

Virtual Server Mapping Parameters:

- Virtual Server 1:

Protocol: TCP
Interface: WAN1
Service Name:
Private IP:
Private Port: 0
Public Port: 0
Schedule: Always
From Day Sunday to Saturday
Time 0 : 0 to 23 : 59

Back Reset Ok

Firewall

"Firewall" - это набор программ, которые защищают ресурсы частной сети. Это позволяет уберечь сеть от несанкционированного вмешательства извне.



Базовый **"Firewall security level"** отвечает за работу NAT firewall и безопасность удаленного управления. NAT firewall становится активным только при разрешенной функции NAT. Безопасное удаленное управление по умолчанию блокирует любое внешнее соединение с устройством. Непустое значение поля "IP pool" в ADMIN вызовет блокировку всех попыток внешнего удаленного управления, за исключением обращений с адресов, попадающих в указанный диапазон.

Home | Basic | Advanced | Status | Admin | Utility

ADVANCED - FIREWALL

Firewall Security Level:

- Firewall security level:

Security Level: Basic Firewall Security

Hint: This level only enables the NAT firewall and the remote management security. The NAT firewall will take effect if NAT function is enabled. The remote management security is default to block any WAN side connection to the device. Non-empty legal IP pool in ADMIN will block all remote management connection except those IPs specified in the pool.

Automatic Firewall Security

Hint: This level enables basic firewall security, all DoS protection, and the SPI filter function.

Advanced Firewall Security

Hint: A user can determine the security level for special purpose, environment, and applications by configuring the DoS protection and defining an extra packet filter with higher priority than the default SPI filter. Note that, an improper filter policy may degrade the capability of the firewall and/or even block the normal network traffic.

Cancel Reset Finish

Нажмите Finish для завершения

На экране будут отображены параметры для записи в EPROM. Проверьте их.

Home | Basic | Advanced | Status | Admin | Utility

ADVANCED - FIREWALL

Firewall Security Level Review:

To let the configuration that you have changed take effect immediately, please click Restart button to reboot the syster procedure, please click Continue button.

- **Firewall security level:**

Security Level	Basic Firewall Security

DoS Protection Parameters Review:

Detect SYN Attack	Disable	SYN Attack Threshold 200 packets per second
Detect ICMP Flood	Disable	ICMP Flood Threshold 200 packets per second
Detect UDP Flood	Disable	UDP Flood Threshold 200 packets per second
Detect PING of Death Attack	Disable	-----
Detect Land Attack	Disable	-----
Detect IP Spoofing Attack	Disable	-----
Detect Smurf Attack	Disable	-----
Detect Fraggle Attack	Disable	-----

Packet Filtering Parameters Review:

- **General packet filtering parameter:**
- **Access policies:**

Index	Enable	Protocol	Direction	Action	Source	Destination	TCP Flag	ICMP Type	Schedule	Description
Pool is Empty !										

Continue Restart

Нажмите Restart для перезапуска устройства или Continue для продолжения установки.

Этот уровень включает все возможности базового, а также DoS защиту, и функцию SPI фильтра.

Home | Basic | Advanced | Status | Admin | Utility

ADVANCED - FIREWALL

Firewall Security Level:

- **Firewall security level:**

Security Level: ○ Basic Firewall Security

Hint: This level only enables the NAT firewall and the remote management security. The NAT firewall will take effect if NAT function is enabled. The remote management security is default to block any WAN side connection to the device. Non-empty legal IP pool in ADMIN will block all remote management connection except those IPs specified in the pool.

◉ Automatic Firewall Security

Hint: This level enables basic firewall security, all DoS protection, and the SPI filter function.

○ Advanced Firewall Security

Hint: A user can determine the security level for special purpose, environment, and applications by configuring the DoS protection and defining an extra packet filter with higher priority than the default SPI filter. Note that, an improper filter policy may degrade the capability of the firewall and/or even block the normal network traffic.

Cancel Reset Finish

Нажмите Finish для завершения.

На экране будут отображены параметры для записи в EPROM. Проверьте их.

Home | Basic | Advanced | Status | Admin | Utility

ADVANCED - FIREWALL

Firewall Security Level Review:

To let the configuration that you have changed take effect immediately, please click Restart button to reboot the syster procedure, please click Continue button.

- **Firewall security level:**

Security Level	Basic Firewall Security

DoS Protection Parameters Review:

Detect SYN Attack	Disable	SYN Attack Threshold 200 packets per second
Detect ICMP Flood	Disable	ICMP Flood Threshold 200 packets per second
Detect UDP Flood	Disable	UDP Flood Threshold 200 packets per second
Detect PING of Death Attack	Disable	-----
Detect Land Attack	Disable	-----
Detect IP Spoofing Attack	Disable	-----
Detect Smurf Attack	Disable	-----
Detect Fraggle Attack	Disable	-----

Packet Filtering Parameters Review:

- **General packet filtering parameter:**

Trigger Packet Filtering Service	Disable

Нажмите Restart для перезапуска устройства или Continue для продолжения установки.

▪ Access policies:

Index	Enable	Protocol	Direction	Action	Source	Destination	TCP Flag	ICMP Type	Schedule	Description
Pool is Empty !										

Continue Restart

Пользователь может использовать специальные правила для задач и приложений путем конфигурирования DoS защиты и дополнительных фильтров с приоритетом выше, чем SPI фильтр.

Home Basic Advanced Status Admin Utility

ADVANCED - FIREWALL

Firewall Security Level:

▪ Firewall security level:

Security Level: ○ Basic Firewall Security

Hint: This level only enables the NAT firewall and the remote management security. The NAT firewall will take effect if NAT function is enabled. The remote management security is default to block any WAN side connection to the device. Non-empty legal IP pool in ADMIN will block all remote management connection except those IPs specified in the pool.

○ Automatic Firewall Security

Hint: This level enables basic firewall security, all DoS protection, and the SPI filter function.

⦿ Advanced Firewall Security

Hint: A user can determine the security level for special purpose, environment, and applications by configuring the DoS protection and defining an extra packet filter with higher priority than the default SPI filter. Note that, an improper filter policy may degrade the capability of the firewall and/or even block the normal network traffic.

Cancel Reset Finish

Предупреждение:неправильно установленный фильтр может уменьшать производительность firewall и даже полностью блокировать нормальный сетевой трафик .

Нажмите Advanced **Firewall Security** и затем нажмите Finish.

Home Basic Advanced Status Admin Utility

FIREWALL - DoS PROTECT

DoS Protect Parameters:

☑ Detect SYN Attack — SYN Attack Threshold 200 packets per second

☑ Detect ICMP Flood — ICMP Flood Threshold 200 packets per second

☑ Detect UDP Flood — UDP Flood Threshold 200 packets per second

☑ Detect PING of Death Attack

☑ Detect Land Attack

☑ Detect IP Spoofing Attack

☑ Detect Smurf Attack

☑ Detect Fraggle Attack

Cancel Reset Finish

SYN flood атаки замедляют работу Вашей сети, запрашивая новые связи, но не заканчивая процесс с уже открытыми соединениями. Как только буфер будет заполнен этими соединениями, сервер не сможет больше устанавливать новые соединения, что приведет к его неработоспособности.

ICMP Flood: Отправитель передает большое количество ICMP запросов для занятия всех ресурсов CPU, которому приходится обслуживать фальшивые запросы.

UDP Flood: Отправитель передает большое количество запросов на UDP диагностический сервис для занятия всех ресурсов CPU, которому приходится обслуживать фальшивые запросы.

Ping of death атаки пытаются вывести из строя Вашу систему путем посылки фрагментов пакетов, в результате чего все ресурсы компьютера уходят на восстановление поврежденных пакетов. Другими известными вариантами атак ping of death являются teardrop, bonk и nestea.

Land атаки пытаются замедлить работу Вашей сети, посылая пакеты с идентичными Вашей сети источниками и адресами назначения.

IP Spoofing атака маскирует вторжение под видом посылки сообщений от разных компьютеров. Это используется злоумышленниками для сохранения анонимности и может применяться в атаках, приводящих к отказу от обслуживания (DoS - Denial of Service attack).

Smurf атаки используют два способа. Атакующий посылает пакеты, содержащие ICMP запросы к сетевым адресам одной системы. Эта система известна как усилитель. Вернувшийся ping адрес является фальшивым (spoofed), будто он прибыл от машины, находящейся в другой сети (жертва). Жертва в результате этого заполняется ping запросами. Так много запросов посылается только для одного нападения, нападающий может использовать много усилителей на машину одной жертвы.

IP Spoofing: Фальсифицирует информацию об IP заголовках для обмана получателя.

Если Вы хотите сконфигурировать Packet Filtering параметры, выберите Enable и нажмите Add.

Home | Basic | Advanced | Status | Admin | Utility

FIREWALL - PKT FILTER

Packet Filtering Parameters:

- General packet filtering parameter:
  Trigger Packet Filtering Service: Disable / Enable
- Access policies:

Index	Enable	Protocol	Direction	Action	Source	Destination	TCP Flag	ICMP Type	Schedule	Description
Pool is Empty !										

Add | Finish

Выберите protocol и сконфигурируйте параметры.

Если Вы хотите запретить все протоколы от IP (т.е.: 200.1.1.1) до получения доступа ко всем PCs (т.е.: 192.168.0.2 ~ 192.168.0.50) в LAN, введите такие параметры:
Protocol: ANY
Direction: INBOUND (INBOUND от WAN в LAN, и OUTBOUND из LAN в WAN.)
Description: Hacker
Src. IP Address: 200.1.1.1
Dest. IP Address: 192.168.0.2-192.168.0.50
Нажмите OK для завершения.

Home | Basic | Advanced | Status | Admin | Utility

PKT FILTER - RULE 1

Packet Filter Rule Parameters:

- Filter rule:
  Protocol: ANY
  Direction: INBOUND / OUTBOUND
  Action: DENY / PERMIT
  Description: Permit for mail server
  Src. IP Address: 0.0.0.0 e.g., Any:0.0.0.0, Single:10.0.0.1
  Dest. IP Address: 192.168.0.111 Range:192.168.0.1-192.168.0.76
  Schedule: Always
  From Day Sunday to Saturday
  Time 0 : 0 to 23 : 59

Back | Cancel | Ok

Home | Basic | Advanced | Status | Admin | Utility

FIREWALL - PKT FILTER

Packet Filtering Parameters:

- General packet filtering parameter:
  Trigger Packet Filtering Service: Disable / Enable
- Access policies:

Index	Enable	Protocol	Direction	Action	Source	Destination	TCP Flag	ICMP Type	Schedule	Description
1	ON	ANY	Inbound	Permit	0.0.0.0 -----	192.168.0.111 -----	---	------	Always	Permit for mail server

Exchange | Modify | Delete | Add | Finish

Экран отобразит настроенные параметры. Проверьте параметры.
Нажмите Restart для перезагрузки шлюза или Continue для формирования других параметров.

Администрирование

Этот раздел включает в себя настройку параметров безопасности, simple network management protocol (SNMP) и time synchronous.

- BASIC
- ADVANCED
- STATUS
- ADMIN
  - SECURITY
  - SNMP
  - TIME SYNC
- UTILITY

Security

Для системной безопасности предлагаем Вам изменить **user name** и **password** в начальных установках для предотвращения доступа к устройству неправомочных пользователей.
Есть три способа настройки: Web browser, telnet и serial console.

Нажмите Security для доступа к настройкам.

- BASIC
- ADVANCED
- STATUS
- ADMIN
  - SECURITY
  - SNMP
  - TIME SYNC
- UTILITY

Для большей безопасности измените Supervisor ID и password для gateway. Если Вы их не установите, каждый пользователь в Вашей сети сможет иметь доступ к устройству, используя default IP и Password root.

Вы можете авторизовать пять пользователей для доступа к маршрутизатору через telnet или console. Существует два UI способа для конфигурации маршрутизатора: menu driven mode и command mode.

Home | Basic | Advanced | Status | Admin | Utility

ADMIN - SECURITY

Supervisor Profile and Security Parameters:

- Supervisor ID and Password:

Supervisor ID: root
Supervisor Password: ****
Password Confirm: ****

- User Profile:

ID	User Name	User Password	Password Confirm	UI Mode
1	admin	*****	*****	Menu
2				Command
3				Command
4				Command
5				Command

- General Parameters:

Telnet Port: 23

Легальный адресный pool позволит установить легальные IP адреса, через которые авторизованные пользователи смогут конфигурировать устройство. Это более безопасная функция для администратора сети по установке легальных адресов.
Конфигурация 0.0.0.0 позволяет всем хостам в интернете иметь доступ к маршрутизатору.

Нажмите Finish для завершения установок.

Браузер отобразит конфигурационные параметры и проверит их перед записью в EPROM.

Нажмите Restart для перезапуска маршрутизатора для работы с новыми параметрами или нажмите Continue для установки других параметров.

- Trust Host List:

Warning: the special trust host IP of 0.0.0.0 allows the access from any hosts on internet.

ID	IP Address
1	0.0.0.0
2	
3	
4	
5	
6	
7	
8	
9	
10	

Cancel Reset Finish

SNMP

Simple Network Management Protocol (SNMP) это протокол не только обеспечивающий сетевое управление, но и позволяющий отслеживать состояние устройств и их функционирование.

Маршрутизатор может генерировать SNMP прерывания для индикации аварийных ситуаций. Он использует SNMP community strings для обеспечения безопасности. Устройство также поддерживает MIB II.

Нажмите SNMP для установки параметров.

- BASIC
- ADVANCED
- STATUS
- ADMIN
  - SECURITY
  - SNMP
  - TIME SYNC
- UTILITY

В таблице "**table of current community pool**", Вы устанавливаете права доступа.

В таблице "**table of current trap host pool**", Вы устанавливаете trap host.

Нажмите Modify для изменения community pool.

Home | Basic | Advanced | Status | Admin | Utility

ADMIN - SNMP

SNMP Community and Trap Parameters:

- Table of current community pool:

Index	Status	Access Right	Community
1	Disable	---	---
2	Disable	---	---
3	Disable	---	---
4	Disable	---	---
5	Disable	---	---

Modify

- Table of current trap host pool:

Index	Version	IP Address	Community
1	Disable	---	---
2	Disable	---	---
3	Disable	---	---
4	Disable	---	---
5	Disable	---	---

Modify

Cancel Finish

SNMP status: Enable

SNMP Community and Trap Parameters:

- **Table of current community pool:**

Index	Status	Access Right	Community
1	Disable / Disable / Enable	Deny	private
2		---	---
3	Disable	---	---
4	Disable	---	---
5	Disable	---	---

Ok Cancel

Access Right: Deny для отвержения любого доступа
Access Right: Read - только для чтения
Access Right: Write - для чтения и записи.
Community: это служит паролем для прав доступа
После конфигурирования нажмите OK.

SNMP Community and Trap Parameters:

- **Table of current community pool:**

Index	Status	Access Right	Community
1	Disable	Deny / Deny / Read / Write	private
2	Disable		---
3	Disable		---
4	Disable	---	---
5	Disable	---	---

Ok Cancel

Нажмите Modify для изменения trap host pool.
Version: выберите version для trap host.
IP: тип trap host IP
Community: тип community password.
Нажмите OK для окончания установок.

- **Table of current trap host pool:**

Index	Version	IP Address	Community
1	Disable / Disable / Version 1 / Version 2	192.168.0.254	private
2		---	---
3		---	---
4	Disable	---	---
5	Disable	---	---

Ok Cancel

Браузер отобразит конфигурационные параметры и проверит их перед записью в EPROM.

Нажмите Restart для перезапуска маршрутизатора для работы с новыми параметрами или нажмите Continue для установки других параметров.

Time Sync

Временная синхронизация является важным элементом для любых применений в IT системах. Причина этого состоит в том, что все системы имеют часы, являющиеся источником времени для файлов или действий с ними. Без синхронизации по времени, время на этих системах изменяется относительно друг друга или относительно правильного времени и это может причинить обработку виртуальных списков сервера системы с неправильными данными.

Home | Basic | Advanced | Status | Admin | Utility

ADMIN - TIME SYNC

Time Synchronization:

- **SYNC method:** Sync with PC (SNTP v4.0 / Sync with PC)
- **Time synchronization with client:**

System Time: 0000/00/00 00:00:00 Sync Now

Нажмите TIME SYNC.

Существует два способа синхронизации: Sample Network Time Protocol (SNTP) и синхронизация с PC. Для синхронизации с PC выберите Sync with PC. Если Вы выбираете синхронизацию с ПК – маршрутизатор синхронизирует с ПК.

SNTP - Simple Network Time Protocol, являющийся адаптацией Network Time Protocol (NTP), использующийся для синхронизации времени в Интернет. SNTP может применяться после полного выполнения NTP.

Для SNTP выберите SNTP v4.0.
SNTP service: Enable
Time Server: Могут использоваться все временные сервера во всем мире, но предлагается использовать сервер, находящийся поблизости.
Time Zone: Вы должны выбрать правильный часовой пояс.

Home | Basic | Advanced | Status | Admin | Utility

ADMIN - TIME SYNC

Time Synchronization:

- SYNC method: SNTP v4.0
- Simple network time protocol:

Service: Disable / Enable
Time Server 1: ntp-2.vt.edu
Time Server 2: ntp.drydog.com
Time Server 2: ntp1.cs.wisc.edu
Time Zone: GMT(-08:00) PACIFIC TIME (US & CANADA); TIJUANA
Update Period (secs): 60

Cancel | Reset | Finish

Нажмите Finish для завершения установок. Браузер отобразит конфигурационные параметры и проверит их перед записью в EPROM.

Сервисные возможности

Этот раздел описывает сервисные функции устройства, включая системную информацию, загрузку конфигурации по умолчанию, обновление системного ПО, и перезапуск маршрутизатора.

- BASIC
- ADVANCED
- STATUS
- ADMIN
- UTILITY
  - SYSTEM INFO
  - CONFIG TOOL
  - UPGRADE
  - RESTART

System Info

Нажмите System Info для просмотра информации.

- BASIC
- ADVANCED
- STATUS
- ADMIN
- UTILITY
  - SYSTEM INFO
  - CONFIG TOOL
  - UPGRADE
  - RESTART

Браузер отобразит системную информацию.

Config Tool

Эта утилита имеет три режима: загрузка заводской конфигурации, восстановление конфигурации и сохранение конфигурации.

BASIC
ADVANCED
STATUS
ADMIN
UTILITY
- SYSTEM INFO
- CONFIG TOOL
- UPGRADE
- RESTART

Нажмите Config Tool.
Выберите режим и нажмите Finish.

- Load Factory Default: загрузит заводские установки по умолчанию.

: Возвратит все установки к заводским, будут потеряны все изменения.

- Restore Configuration: Иногда происходит непредвиденное разрушение конфигурации. Этот режим позволяет восстановить ее из ранее записанной.

✧ Нажмите Finish после выбора.
✧ Укажите место хранения и нажмите Finish. Сохраненная конфигурация будет восстановлена.

- Backup Configuration: После завершения конфигурации позволяет сохранить ее на Вашем компьютере.

✧ Выберите "Backup Configuration" и нажмите Finish.
✧ Укажите место для хранения файла. Нажмите Finish. Конфигурация будет сохранена.

Home | Basic | Advanced | Status | Admin | Utility

UTILITY - CONFIGURATION TOOL

Select Configuration Tool:

Configuration Tool: Load Factory Default
Load Factory Default
Restore Configuration
Backup Configuration

Finish

Upgrade

Вы можете обновить системное ПО Вашего маршрутизатора при помощи этой функции.
Нажмите Upgrade.

BASIC
ADVANCED
STATUS
ADMIN
UTILITY
- SYSTEM INFO
- CONFIG TOOL
- UPGRADE
- RESTART

Укажите файл и нажмите OK - система перезапустится автоматически по завершении обновления.

Home | Basic | Advanced | Status | Admin | Utility

UTILITY - FIRMWARE UPGRADE

Firmware Upgrade:
Please select the firmware file that you want, and press Ok button to upgrade the system, then the system will restart a

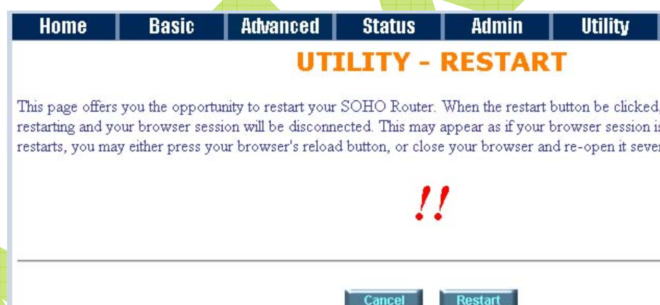
Browse...

Cancel Ok

Restart

Для перезапуска маршрутизатора нажмите Restart .

Нажмите Restart для перезапуска.



Статус

Вы можете контролировать состояние SHDSL-соединения, включая контроль Tx, контроль Bitrate и информацию о состоянии SNR, CRC ошибки.

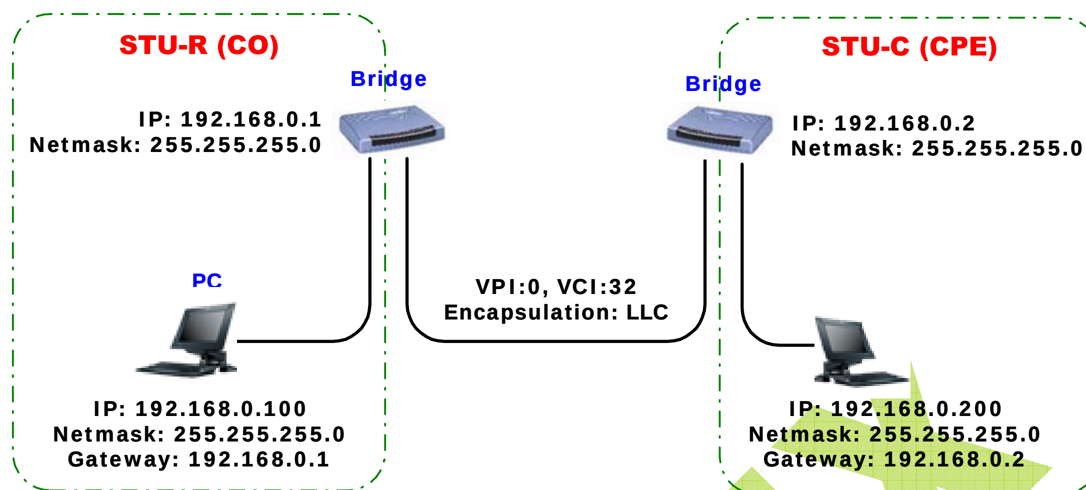
LAN status отображает информацию о состоянии MAC адресов, IP адресов, Subnet mask и таблицу для DHCP client.

WAN status показывает информацию о состоянии WAN интерфейса.

Вы можете посмотреть таблицу маршрутизации и состояния маршрута.

Interface status отображает статистическую информацию о LAN и WAN интерфейсах.

LAN-to-LAN соединение в режиме bridge



CO side

Нажмите Bridge и CO для установки режима «**bridge**» и затем нажмите Next.

LAN параметры
Введите IP: 192.168.0.1
Введите Subnet Mask: 255.255.255.0
Введите Gateway: 192.168.0.1
Введите Host Name: SOHO

WAN1 параметры
Введите VPI: 0
Введите VCI: 32
Нажмите LLC
Нажмите Next

Экран отобразит новые сконфигурированные параметры.
Проверьте параметры и нажмите Restart.
Маршрутизатор будет перенастроен с учетом новых установок.

CPE Side

Нажмите Bridge и CO для установки режима «**bridge**» и затем нажмите Next.

LAN параметры
Введите IP: 192.168.0.2
Введите Subnet Mask: 255.255.255.0
Введите Gateway: 192.168.0.2
Введите Host Name: SOHO

WAN1 параметры
Введите VPI: 0
Введите VCI: 32
Нажмите LLC
Нажмите Next

Экран отобразит новые сконфигурированные параметры. Проверьте параметры и нажмите Restart. Маршрутизатор будет перенастроен с учетом новых установок.

Поздравляем! Вы закончили.
Ваше LAN-to-LAN SHDSL соединение установлено.

Конфигурация через консольный порт или Telnet

Serial Console

Проверьте возможность соединения RS-232 кабелем Вашего компьютера и последовательного порта маршрутизатора. Начните Вашу терминальную программу доступа с настройки эмуляции терминала VT100. Сконфигурируйте последовательную связь с параметрами: baudrate 9600, 8 data bits, no parity check, 1 stop bit, and no flow-control и нажмите SPACE до появления login экрана. После появления login экрана Вы будете иметь доступ к управлению маршрутизатором.

```
User: admin
Password: *****
```

Внимание: Если Вы не установили никакого пользовательского профиля на своем маршрутизаторе, введите в поле «user» фабричный профиль «admin». Когда система запросит у Вас пароль, введите «admin» для доступа к маршрутизатору.

Telnet

Удостоверьтесь, что используется правильный Ethernet кабель для соединения LAN портов Вашего компьютера и маршрутизатора. При использовании правильного Ethernet кабеля LAN LNK индикатор на передней панели должен загореться. Начните установку Telnet клиента с эмуляции терминала VT100 и соединения с IP управления маршрутизатором, ждите до появления login экрана. После появления login экрана Вы будете иметь доступ к управлению маршрутизатором.

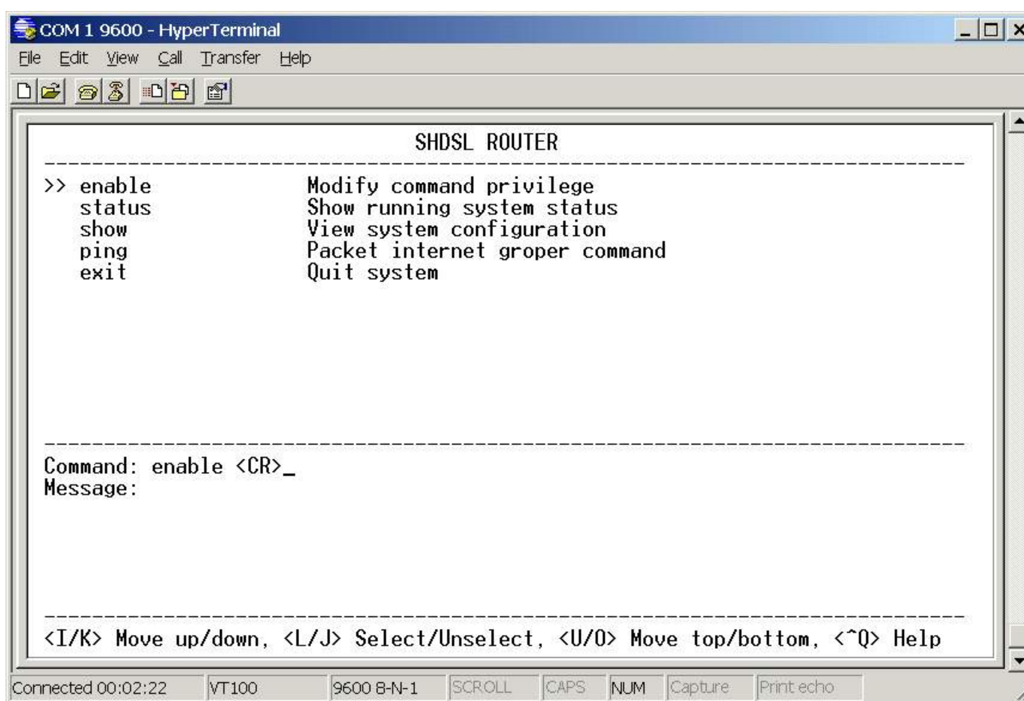
```
User: admin
Password: *****
```

Внимание: Если Вы не установили никакого LAN IP адреса на маршрутизаторе, то по умолчанию IP адрес будет 192.168.0.1.

Operation Interface

Для управления при помощи консольного порта или по Telnet, маршрутизатор имеет два интерфейса: интерфейс командной строки (CLI) и меню управляемый интерфейс. CLI обеспечивает пользователю простой интерфейс, который лучше всего использовать для работы со script файлами. Меню управляемый интерфейс является легким в использовании интерфейсом для общих операций. Синтаксис команд для CLI является таким же, как и для меню управляемого интерфейса. Единственное различие между ними в том, что меню управляемый интерфейс показывает Вам все доступные для выбора команды. Вам не нужно запоминать синтаксис команд, и Вы можете сэкономить время при вводе целой командной строки.

Следующая диаграмма показывает Вам пример меню управляемого интерфейса. В меню Вы можете передвигаться вверх/вниз при помощи нажатия кнопок I / K, выбрать одну из команд кнопкой L и вернуться к верхнему уровню меню при помощи кнопки J. Например, чтобы показать системную информацию маршрутизатора, переместите курсор вниз нажатием кнопки K дважды и выберете команду “**show**” при помощи кнопки L, Вы увидите подменю, в котором выберите команду “**system**”, после этого система покажет Вам основную информацию.



Window structure

Сверху вниз, окно будет разделено на четыре части:

1. Наименование изделия
2. Поле меню: в этом поле отображено дерево. Символ “**>>**” указывает место курсора.
3. Поле конфигураций: В этом поле вы можете конфигурировать параметры. **< parameters >** показывает параметры, которые Вы можете выбрать; **< more…>** указывает на подменю в заголовке.
4. Помощь.

Menu Driven Interface Commands

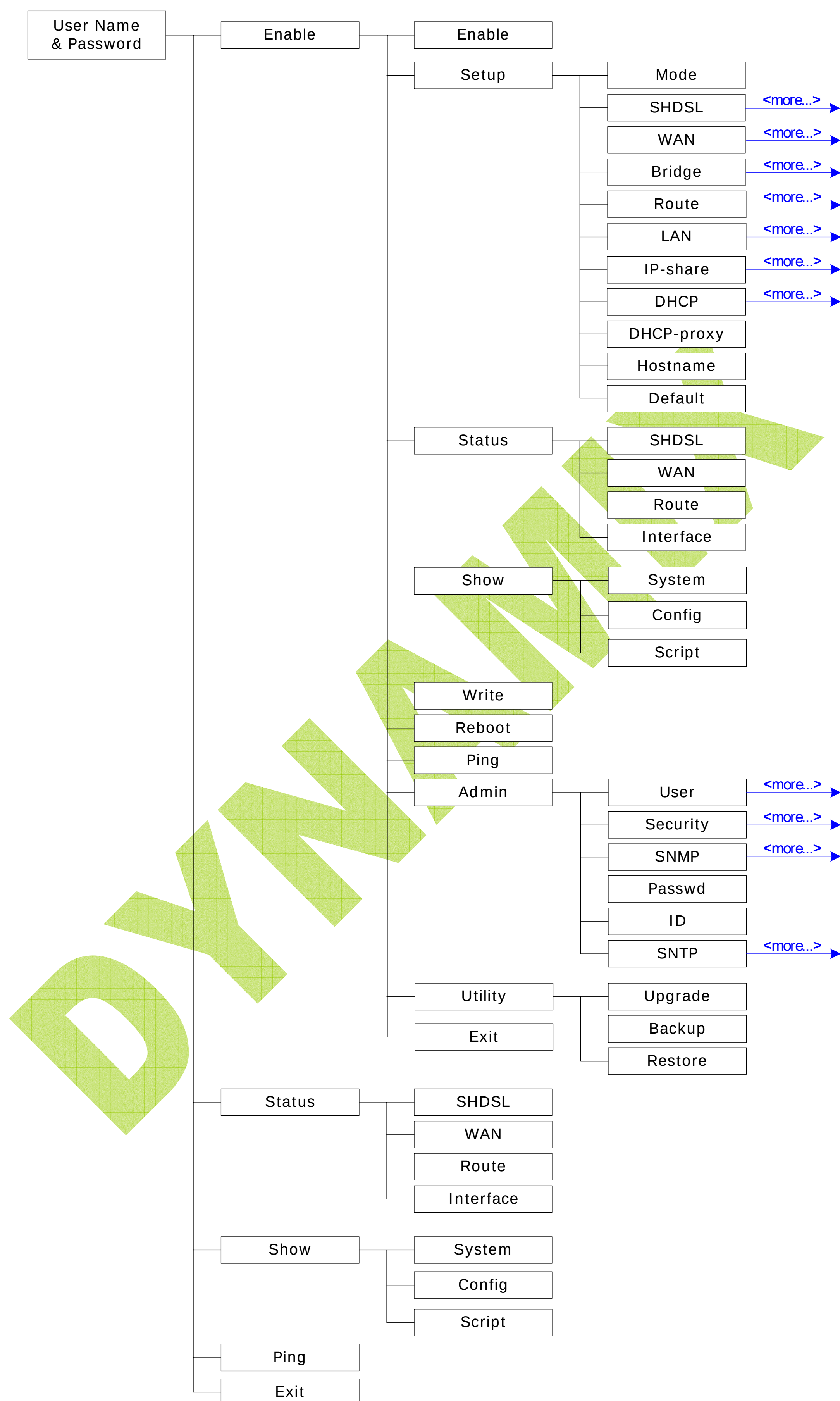
После изменения конфигурации, ознакомьтесь со списком операций в следующей таблице. Список операций будет показан в окне.

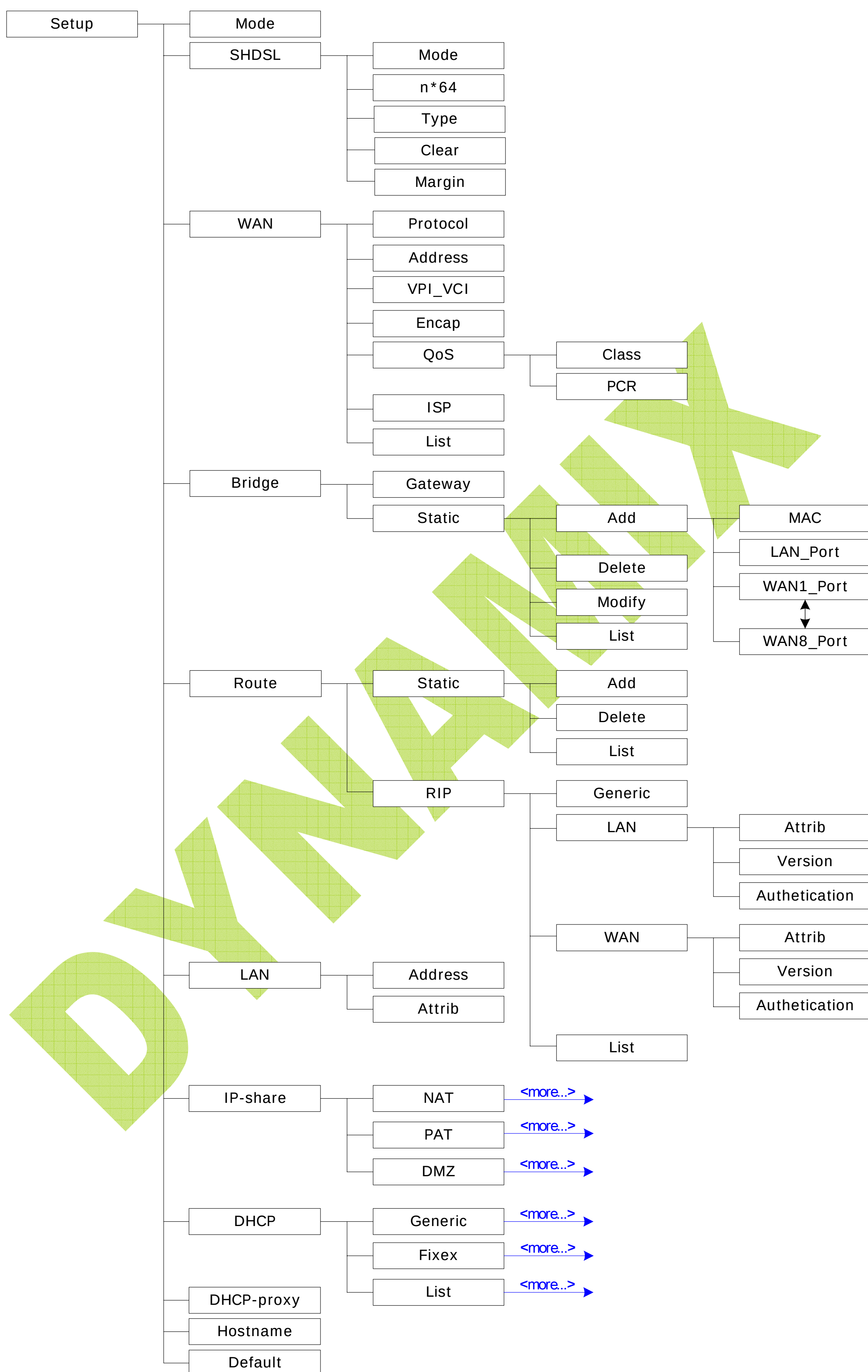
Команды меню управляемого интерфейса

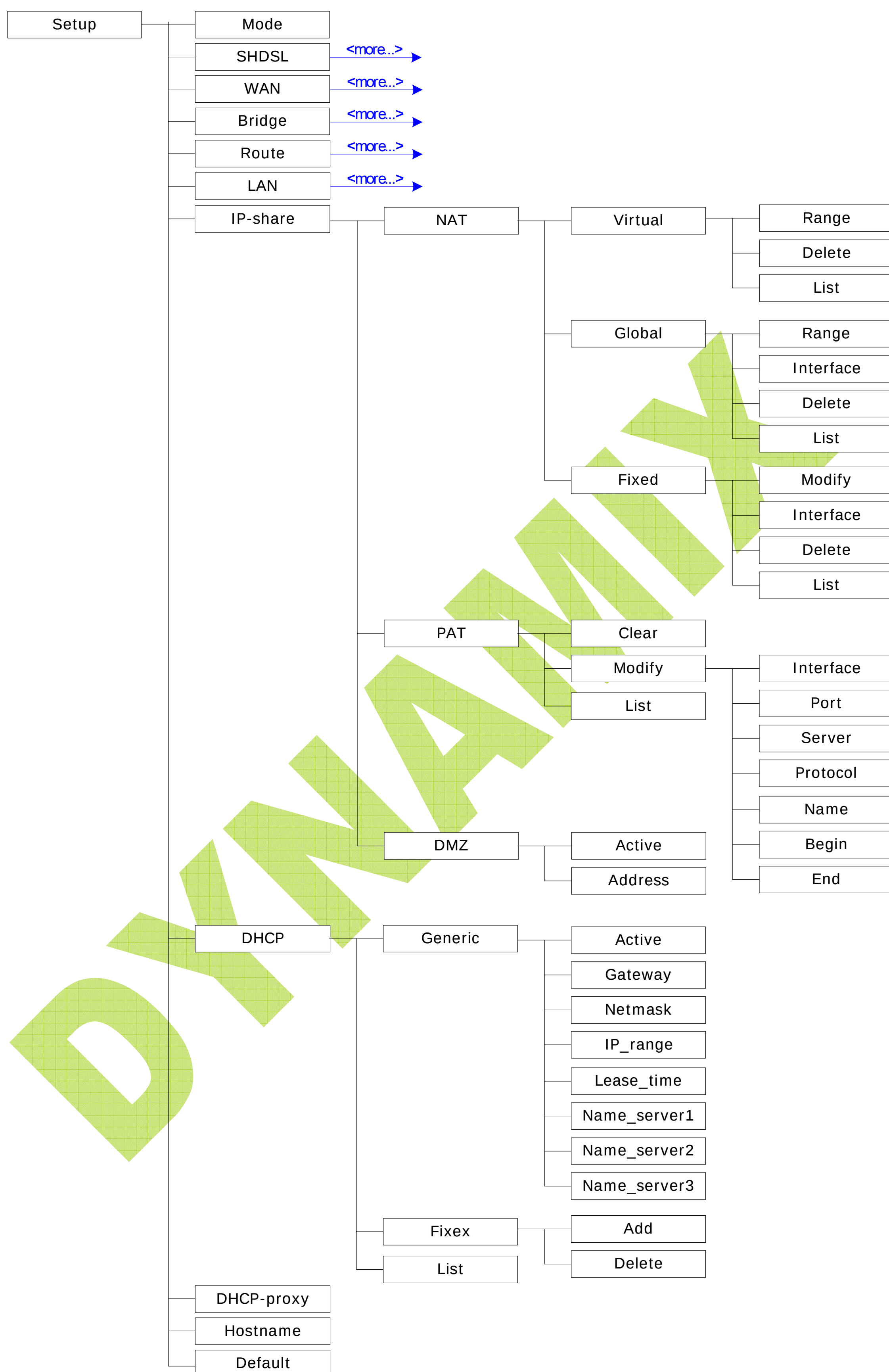
Клавиши	Описание
[UP] или I	Переход в верхнее поле в том же уровне меню.
[DOWN] или K	Переход в нижнее поле в том же уровне меню.
[LEFT] или J	Возвращение к предыдущему меню.
[RIGHT] или L	Переход к подменю.
[ENTER]	Переход к подменю.
[TAB]	Выбор других параметров.
Ctrl + C	Выход из конфигурационного меню.
Ctrl + Q	Помощь.

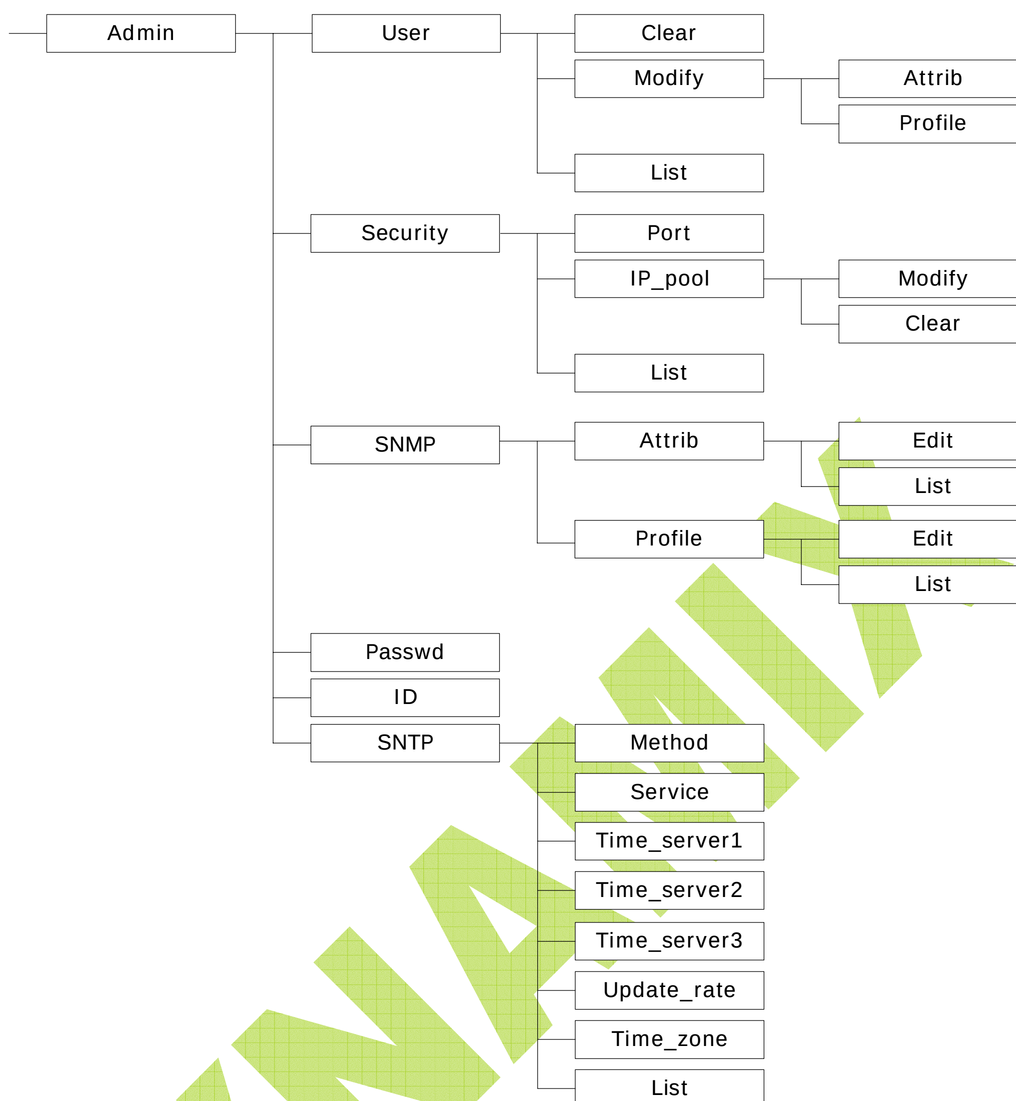
Menu Tree

Все команды помещены в подсправочники («дерево меню»), которые могут быть защищены паролем. Неправомочный пользователь не может изменить никаких конфигурационных настроек, но имеет возможность использовать ping-команды, чтобы удостовериться, что маршрутизатор работает.


User Name
& Password
Enable
Enable
Setup
Mode
SHDSL
WAN
Bridge
Route
LAN
IP-share
DHCP
DHCP-proxy
Hostname
Default
<more...>
Status
SHDSL
WAN
Route
Interface
Show
System
Config
Script
Write
Reboot
Ping
Admin
User
Security
SNMP
Passwd
ID
SNTP
Utility
Upgrade
Backup
Restore
Exit
Status
SHDSL
WAN
Route
Interface
Show
System
Config
Script
Ping
Exit


Setup
Mode
SHDSL
Mode
n*64
Type
Clear
Margin
WAN
Protocol
Address
VPI_VCI
Encap
QoS
Class
PCR
ISP
List
Bridge
Gateway
Static
Add
MAC
LAN_Port
WAN1_Port
WAN8_Port
Delete
Modify
List
Route
Static
Add
Delete
List
RIP
Generic
LAN
Attrib
Version
Authetication
WAN
Attrib
Version
Authetication
List
LAN
Address
Attrib
IP-share
NAT
<more..>
PAT
<more..>
DMZ
<more..>
DHCP
Generic
<more..>
Fixex
<more..>
List
<more..>
DHCP-proxy
Hostname
Default


Setup
Mode
SHDSL
WAN
Bridge
Route
LAN
<more..>
<more..>
<more..>
<more..>
<more..>
IP-share
NAT
Virtual
Range
Delete
List
Global
Range
Interface
Delete
List
Fixed
Modify
Interface
Delete
List
PAT
Clear
Modify
List
Interface
Port
Server
Protocol
Name
Begin
End
DMZ
Active
Address
DHCP
Generic
Active
Gateway
Netmask
IP_range
Lease_time
Name_server1
Name_server2
Name_server3
Fixex
Add
Delete
List
DHCP-proxy
Hostname
Default
DYNAMIX



Конфигурация

Для доступа к маршрутизатору, переместите курсор“ **>>**” в «**enable»** и нажмите любую клавишу. Когда появится экран, введите пароль пользователя. Пароль по умолчанию **-root**. Пароль будет отображен символами “ * “ для системной безопасности.

```
----------------------------------------------------------------------
Command: enable <CR>
Message: Please input the following information.

Supervisor password: ****
----------------------------------------------------------------------
```

В этом подменю, Вы можете установить: параметры управления и модернизировать программное обеспечение, резервные системные конфигурации и восстановить системные конфигурации через сервисные инструменты.

Для безопасности системы предлагается изменить имя пользователя и пароль после начальных установок. После изменения имени пользователя и пароля, настоятельно рекомендуем Вам их хорошо запомнить, так как в дальнейшем Вы будете пользоваться только этим именем пользователя и паролем. Для любых изменений, Вы должны записать новые конфигурации в EPROM и перезагрузить маршрутизатор для работы с новыми установками.

Экран будет показывать следующее.

```
---------------------------------------------------------------------------
>> enable         Modify command privilege
   setup          Configure system
   status         Show running system status
   show           View system configuration
   write          Update flash configuration
   reboot         Reset and boot system
   ping           Packet internet groper command
   admin          Setup management features
   utility        TFTP upgrade utility
   exit           Quit system
---------------------------------------------------------------------------
```

Status

Вы можете посмотреть состояние SHDSL, WAN, состояние маршрутизации и интерфейсов при помощи команды «**status**».

Переместите курсор “ **>>** “ в «**status»** и нажмите enter.

```
---------------------------------------------------------------------------
>> shdsl          Show SHDSL status
   wan            Show WAN interface status
   route          Show routing table
   interface      Show interface statistics status

---------------------------------------------------------------------------
```

Show

Вы можете посмотреть системную информацию и конфигурации при помощи команды «**show»**.

Переместите курсор “ **>>** “ в «**show»** и нажмите enter.

```
---------------------------------------------------------------------------
>> system         Show general information
   config         Show all configuration
   script         Show all configuration in command script

---------------------------------------------------------------------------
```

Write

Для любых изменений в конфигурациях Вам нужно записать новые конфигурации в EPROM, используя команду «**write»** и перезагрузить маршрутизатор для работы с новыми настройками.

Переместите курсор “ **>>** “ в «**write»** и нажмите enter.

```
----------------------------------------------------------------------
Command: write <CR>
Message: Please input the following information.

Are you sure? (y/n): y
----------------------------------------------------------------------
```

Reboot

Для перезагрузки маршрутизатора используйте команду «**reboot»**.

Переместите курсор “ **>>** “ в «**reboot»** и нажмите enter.

```
----------------------------------------------------------------------
Command: reboot <CR>
Message: Please input the following information.

Do you want to reboot? (y/n): y
----------------------------------------------------------------------
```

Ping

Команда **Ping** используется для проверки связи маршрутизатора.
Переместите курсор “ **>>** “ в «**ping**» и нажмите enter.

```
-----------------------------------------------------------------------
Command: ping <ip> [1~65534|-t] [1~1999]
Message: Please input the following information.

IP address <IP> : 10.0.0.1
Number of ping request packets to send (TAB select): 1~65534
Data size [1~1999]: 32
-----------------------------------------------------------------------
```

Administration

Вы можете изменять пользовательский профиль, следить за передаваемой информацией, поддержка telnet доступа, SNMP (Sample Network Management Protocol), SNTP (Simple Network Time Protocol) с помощью команды «**admin**». Маршрут «**enable» ➔ «admin»**.

Для конфигурации параметров, переместите курсор “ **>>** “ в «**admin**» и нажмите enter.

```
-----------------------------------------------------------------------
>> user         Manage user profile
   security     Setup system security
   snmp         Configure SNMP parameter
   passwd       Change supervisor password
   Id           Change supervisor ID
   sntp         Configure time synchronization
-----------------------------------------------------------------------
```

User Profile

Вы можете использовать команду «**user**» для очистки, модификации и просмотра. Вы можете подключать до пяти пользователей для доступа к маршрутизатору через консольный порт или по telnet в таблице пользовательских профилей, однако пользователи, имеющие пароль могут изменить конфигурации маршрутизатора.
Переместите курсор “ **>>** “ в «**user**» и нажмите enter.

```
-----------------------------------------------------------------------
>> clear        Clear user profile
   modify       Modify the user profile
   list         List the user profile
-----------------------------------------------------------------------
```

Вы можете удалять пользователей, используя команду «**clear**». Если Вы не уверены в количестве пользователей, Вы можете использовать команду «**list**» для проверки их количества. Команда «**Modify**» позволяет менять старую информацию или добавлять нового пользователя в пользовательские профили.

Security

Команды безопасности помогут сформировать десять легальных IP адресов для доступа по telnet и номеру порта.

Переместите курсор “ **>>** “ в «**security**» и нажмите enter. Адрес, установленный по умолчанию 0.0.0.0. Это обозначает, что нет никаких IP ограничений для доступа к маршрутизатору через telnet.

```
-----------------------------------------------------------------------
>> port         Configure telent TCP port
   ip_pool      Legal address IP address pool
   list         Show security profile
-----------------------------------------------------------------------
```

SNMP

Simple Network Management Protocol (SNMP) является не только сетевым протоколом управления, он также используется для мониторинга сетевых устройств и их функционирования.

Маршрутизатор может генерировать SNMP прерывания для индикации аварийных ситуаций. Он использует SNMP community strings для обеспечения безопасности. Устройство также поддерживает MIB II.

Переместите курсор “ **>>** “ в «**snmp»** и нажмите enter.

```
>> community      Configure community parameter
   trap           Configure trap host parameter
```

Supervisor Password and ID

Пароль пользователя и ID являются последними и самыми важными инструментами для обеспечения безопасности. Пользователи, которые имеют доступ к маршрутизатору через web-браузер, консольный порт или по telent должны использовать ID и пароль для конфигурации маршрутизатора. Советуем сразу изменить ID и пароль.

SNTP

Временная синхронизация является важным элементом для любых применений в IT системах. Причина этого состоит в том, что все системы имеют часы, являющиеся источником времени для файлов или действий с ними. Без синхронизации по времени, время на этих системах изменяется относительно друг друга или относительно правильного времени и это может причинить обработку виртуальных списков сервера системы с неправильными данными.

Существует два способа синхронизации времени: синхронизировать с ПК или SNTPv4. Если Вы выбираете синхронизацию с ПК – маршрутизатор синхронизирует с ПК. Если Вы выбираете SNTPv4, маршрутизатор будет использовать протокол синхронизации с временным сервером.

Переместите курсор “ **>>** “ в «**sntp»** и нажмите enter.

```
>> method         Select time synchronization method
   service        Tigger SNTP v4.0 service
   time_server1   Configure time server 1
   time_server2   Configure time server 2
   time_server3   Configure time server 3
   updaterate     Configure update period
   time_zone      Configure GMT time zone offset
   list           Show SNTP configuration
```

Utility

Существует три сервисных инструмента: модернизация, резервирование и восстановление, встроенные в программируемое оборудование. Вы можете модернизировать новое программное обеспечение через TFTP инструменты модернизации, создать резервные конфигурации при помощи TFTP резервных инструментов, восстановить конфигурации через TFTP инструменты восстановления. Модернизация TFTP сервера с новым программируемым оборудованием поддерживается поставщиком, для резервирования и восстановления Вы должны иметь собственный TFTP сервер для резервирования и восстановления файлов.

Переместите курсор “ **>>** “ в «**utility»** и нажмите enter.

```
>> upgrade        Upgrade main software
   backup         Backup system configuration
   Restore        Restore system configuration
```

Exit

Если Вы хотите выйти из системы без сохранения, используйте команду «**exit»** для выхода.

Setup

Все установочные параметры расположены в подсправочниках для установки.
Переместите курсор “ **>>** “ в «**setup»** и нажмите enter.

```
>> mode           Switch system operation mode
   shdsl          Configure SHDSL parameters
   wan            Configure WAN interface profile
   bridge         Configure transparent bridging
   route          Configure routing parameters
   lan            Configure LAN interface profile
   ip_share       Configure NAT/PAT parameters
   dhcp           Configure DHCP parameters
   dns_proxy      Configure DNS proxy parameters
   hostname       Configure local host name
   default        Restore factory default setting
```

Mode

Изделие может работать как в режиме моста, так и маршрутизатора. В первоначальных установках установлен режим маршрутизатора. Вы можете изменить режим работы устройства при помощи «**mode»** команд.
Переместите курсор “ **>>** “ в «**mode»** и нажмите enter.

```
Command: setup mode <Route|Bridge>
Message: Please input the following information.

System operation mode (TAB select) <Route>: Route
```

SHDSL

Вы можете установить SHDSL параметры с использованием команды «**shdsl»**.
Переместите курсор “ **>>** “ в «**shdsl»** и нажмите enter.

```
>> mode           Configure SHDSL mode
   n*64           Configure SHDSL data rate
   type           Configure SHDSL annex type
   clear          Clear current CRC error count
   margin         Configure SHDSL SNR margin
```

Существует два типа SHDSL режимов: STU-R и STU-C. STU-R используется как терминал центрального офиса, STU-C – как оборудование клиентской части.

Вы можете установить скорость передачи nx64Kbps при n= 0…32. Если Вы установите n=0, изделие будет работать в режиме адаптации.

Существует два типа SHDSL Annex : Annex-A и Annex-B.

Команда «**clear»** исправляет CRC ошибки.

Вам не нужно изменять SNR, если диапазон от 0 до 10.

WAN

Маршрутизатор поддерживает 8 PVC (private virtual circuit) и Вы можете установить до 8 WAN: от WAN1 до WAN8.
Переместите курсор “ **>>** “ в «**wan»** и нажмите enter. Установится WAN1, type **1**.

```
-----------------------------------------------------------------------
Command: setup wan <1~8>
Message: Please input the following information.

Interface number <1~8>: 1
-----------------------------------------------------------------------
```

```
>> protocol      Link type protocol
   address       IP address and subnet mask
   vpi_vci       Configure VPI/VCI value
   encap         Configure encapsulation type
   qos           Configure VC QoS
   isp           Configure account name, password and idle time
   list          WAN interface configuration
```

Есть четыре типа протоколов: IPoA, EoA, PPPoA и PPPoE, которые поддерживаются ISP.

Для PPPoA и PPPoE Вам не нужно устанавливать IP адрес и subnet mask.

Есть уникальный VPI и VCI для соединения с Интернет, которые поддерживает Ваш ISP. Диапазон VIP от 0 до 255, диапазон VCI от 0 до 65535.

Существует два типа инкапсуляции: VC-Mux и LLC.

Вы можете установить качество обслуживания VC QoS, используя команду «**qos»**. Существует два класса QoS: UBR и CBR. Пиковый разряд может формироваться на скоростях от 64kbps до 2400kbps.

Команда ISP может конфигурировать account name, password и idle time. Idle time может быть от 0 минут до 300 минут.

Вы можете просмотреть конфигурации WAN интерфейса при помощи команды «**list»**.

Bridge

Вы можете настроить параметры работы в режиме моста, используя команду «**bridge»**. Если изделие конфигурируется в режиме маршрутизатора, Вам не нужно настраивать «**bridge»** параметры.
Переместите курсор “ **>>** “ в «**bridge»** и нажмите enter.

```
>> gateway       Default gateway
   static        Static bridging table
```

Вы можете настроить gateway IP, используя команду «**gateway»**.

Вы можете установить 20 статических путей в режиме моста, используя команду «**static»**.

Route

Вы можете настроить параметры работы в режиме маршрутизатора, используя команду

«route». Если изделие конфигурируется в режиме моста, Вам не нужно настраивать **«route»** параметры.
Переместите курсор “ **>>** “ в **«route»** и нажмите enter.

```
--------------------------------------------------------------------------
>> static          Configure static routing table
   RIP             Configure RIP tool

--------------------------------------------------------------------------
```

Вы можете установить 20 статических путей в режиме маршрутизатора, используя команду **«static»**.

Для получения большей информации о RIP, смотрите обзор маршрутизации на странице 16.

LAN

```
--------------------------------------------------------------------------
>> address         LAN IP address and subnet mask
   attrib          NAT network type

--------------------------------------------------------------------------
```

IP share

```
--------------------------------------------------------------------------
>> nat             Configure network address translation
   pat             Configure port address translation
   dmz             Configure DMZ host function

--------------------------------------------------------------------------
```

Для большей информации о NAT, PAT и DMZ, смотрите обзор NAT/DMZ на странице 18.

DHCP

```
--------------------------------------------------------------------------
>> generic         Configure generic DHCP parameter
   Fixed           Configure fixed host IP address list
   list            Show DHCP configuration

--------------------------------------------------------------------------
```

Для большей информации о DHCP, смотрите обзор DHCP на странице 10.

DNS proxy

Вы можете установить три DNS сервера на своем изделии. DNS сервера номер 2 и 3 идут как опция.
Переместите курсор “ **>>** “ в **«dns_proxy»** и нажмите enter.

```
----------------------------------------------------------------------
Command: setup dns_proxy <IP> [IP] [IP]
Message: Please input the following information.

DNS server 1 (ENTER for default) <168.95.1.1>: 10.0.10.1
DNS server 2: 10.10.10.1
DNS server 3:
----------------------------------------------------------------------
```

Host name

Вы можете настроить имя хоста, используя команду **«hostname»**.
Переместите курсор “ **>>** “ в **«hostname»** и нажмите enter.

```
-----------------------------------------------------------------------
Command: setup hostname <name>
Message: Please input the following information.

Local hostname (ENTER for default) <SOHO>: test

-----------------------------------------------------------------------
```

Default

Если Вы хотите восстановить установки по умолчанию, сначала переместите курсор “ **>>** “ в «**default»** и потом нажмите enter.

```
-----------------------------------------------------------------------
Command: setup default <name>
Message: Please input the following information.

Are you sure? (Y/N): y
```